2010-12

Optimizing security of cloud computing within the DoD

Antedomenico, Noemi

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

OPTIMIZING SECURITY OF CLOUD COMPUTING WITHIN THE DOD

by

Noemi Antedomenico

December 2010

Thesis Co-Advisors: Dorothy E. Denning
Ted Lewis
James Bret Michael

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Optimizing Security of Cloud Computing within the DoD			**5. FUNDING NUMBERS**
6. AUTHOR(S) Noemi Antedomenico			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** **A**

13. ABSTRACT (maximum 200 words)

What countermeasures best strengthen the confidentiality, integrity and availability (CIA) of the implementation of cloud computing within the DoD? This question will be answered by analyzing threats and countermeasures within the context of the ten domains comprising the Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK). The ten domains that will be used in this analysis include access control; telecommunications and network security; information security governance and risk management; application security; cryptography; security architecture and design; operations security; business continuity planning and disaster planning; legal regulations, compliance, and investigation; and physical security. The results of this research provide a comprehensive guide for any DoD entity attempting to secure its cloud solution.

14. SUBJECT TERMS Cloud computing, Information Security of Cloud Computing, Computer Security with Cloud Computing, Information System Security with Cloud Computing, CISSP and Cloud Computing			**15. NUMBER OF PAGES** 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

OPTIMIZING SECURITY OF CLOUD COMPUTING WITHIN THE DOD

Noemi Antedomenico
Major, United States Air Force
B.S., United States Air Force Academy, 1997
M.A., Bowie State University, 2001
MBA, University of West Florida, 2009

Submitted in partial fulfillment of the
Requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Noemi Antedomenico

Approved by: Dorothy E. Denning
Thesis Co-Advisor

Ted Lewis
Thesis Co-Advisor

James Bret Michael
Thesis Co-Advisor

Harold Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

What countermeasures best strengthen the confidentiality, integrity and availability (CIA) of the implementation of cloud computing within the DoD? This question will be answered by analyzing threats and countermeasures within the context of the ten domains comprising the Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK). The ten domains that will be used in this analysis include access control; telecommunications and network security; information security governance and risk management; application security; cryptography; security architecture and design; operations security; business continuity planning and disaster planning; legal regulations, compliance, and investigation; and physical security. The results of this research provide a comprehensive guide for any DoD entity attempting to secure its cloud solution.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- **A. MAJOR RESEARCH QUESTION....1**
- **B. IMPORTANCE....1**
- **C. PROBLEMS AND HYPOTHESIS....2**
  - **1. Cloud Vulnerability....4**
    - ***a. Hacked....4***
    - ***b. Outage....4***
    - ***c. Data Loss....5***
  - **2. Addressing the Vulnerability....5**
- **D. METHODS AND SOURCES....6**
- **E. OVERVIEW OF THESIS....6**

II. LITERATURE REVIEW....7
- **A. WHAT IS CLOUD COMPUTING?....7**
- **B. PROS AND CONS TO CLOUD COMPUTING....8**
- **C. CLOUD COMPUTING DEPLOYMENT MODELS....9**
  - **1. Public Cloud....9**
  - **2. Private Cloud....10**
  - **3. Community Cloud....10**
  - **4. Hybrid Cloud....11**
  - **5. Private Cloud Recommended by DoD....11**
- **D. CLOUD COMPUTING SERVICE MODELS....12**
  - **1. Infrastructure as a Service (IaaS)....12**
  - **2. Platform as a Service (PaaS)....12**
  - **3. Software as a Service (SaaS)....13**
  - **4. Security Tradeoffs between Service Models....13**
- **E. WHAT IS CURRENT IN THE DOD?....14**
  - **1. Army Experience Center (AEC)....14**
  - **2. Rapid Access Computing Environment (RACE)....14**
  - **3. Forge.mil....15**
  - **4. Personnel Services Delivery Transformation (PSDT)....16**
- **F. JUSTIFICATION FOR THE TEN DOMAINS....16**
- **G. DESCRIPTIONS OF THE TEN DOMAINS....17**
  - **1. Access Control....17**
  - **2. Telecommunications and Network Security....18**
  - **3. Information Security Governance and Risk Management....18**
  - **4. Application Security....19**
  - **5. Cryptography....19**
  - **6. Security Architecture and Design....20**
  - **7. Operational Security (OPSEC)....20**
  - **8. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)....20**

9. Legal Regulations, Compliance, and Investigation.....21
10. Physical and Environmental Security.....21
H. SECURITY ADVANTAGES TO CLOUD COMPUTING.....21
I. SECURITY CHALLENGES WITH CLOUD COMPUTING.....23
III. THE FUTURE OF CLOUD.....27
V. DISSECTING THE TEN DOMAINS.....33
Introduction: Inherent Risk with External Providers.....33
1. Access Control.....33
2. Telecommunications and Network Security.....37
3. Information security governance and risk management.....42
4. Application Security.....49
5. Cryptography.....52
6. Security Architecture and Design.....57
7. Operational Security.....59
8. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP).....64
9. Legal Regulations, Compliance and Investigation.....67
10. Physical and Environmental Security.....73
VI. CONCLUSION.....78
LIST OF REFERENCES.....81
INITIAL DISTRIBUTION LIST.....91

LIST OF FIGURES

Figure 1. Overarching Cloud Computing Governance Resources 44

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AEC	Army Experience Center
AFPC	Air Force Personnel Center
API	Application Programming Interface
BCP	Business Continuity Plan
BEP	Bureau of Engraving and Printing
CANES	Consolidated Afloat Network Enterprise System
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CBK	Common Body of Knowledge
CERT	Computer Emergency Response Team
CIA	confidentiality, integrity and availability
CIO	Chief Information Officer
CISSP	Certified Information System Security Professional
CSA	Cloud Security Alliance
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoS	Denial of Service
DRP	Disaster Recovery Plan
ENISA	European Network and Information Security Agency
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information System Management Act
GAO	Government Accountability Office
HVAC	Heating, Ventilation, and Air-Conditioning
IA	Information Assurance
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IPS	Intrusion Protection System
(ISC)2	International Information System Security Certification Consortium

ISIMC	Information Security and Identity Management Committee
ISR	Intelligence Surveillance and Reconnaissance
IT	Information Technology
NAC	Network Access Control
NGEN	Next Generation Enterprise Network
NIST	National Institute of Standards and Technology
OATH	Open Authentication
OPSEC	Operational Security
PaaS	Platform as a Service
PSDT	Personnel Services Delivery Transformation
RACE	Rapid Access Computing Environment
RTO	Recovery Time Objectives
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SPML	Service Provisioning Mark-up Language
SSH	Secure Shell
SSO	Single Sign On
TCP/IP	Transmission Control Protocol/Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network

ACKNOWLEDGMENTS

Thank you to my thesis advisors, Dr. Dorothy E. Denning, Dr. Ted Lewis, and Dr. Bret Michael, for their assistance and time on this product.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MAJOR RESEARCH QUESTION

What countermeasures best strengthen the confidentiality, integrity and availability (CIA) of the implementation of cloud computing[1] within the DoD? This question will be answered by analyzing threats and countermeasures within the context of the ten domains comprising the Certified Information System Security Professional (CISSP) Common Body of Knowledge (CBK). The ten domains that will be used in this analysis include access control, telecommunications and network security, information security governance and risk management, application security, cryptography, security architecture and design, operations security, business continuity planning and disaster planning; legal regulations, compliance, and investigation; and physical security.[2] The results of this research provide a comprehensive guide for any DoD entity attempting to secure its cloud solution.

B. IMPORTANCE

A vital DoD interest is to protect its information systems to ensure the CIA of critical data at home and abroad. In order to protect DoD information infrastructures within the context of cloud computing, the tactics and insight of network security professionals on both threats and corresponding countermeasures provide invaluable references necessary for deterring malicious attacks from U.S. adversaries.

The Obama Administration is encouraging a push for agencies to implement cloud computing when operational efficiencies and financial benefits are evident.[3] This push is accompanied with a requirement for cyber security. On May 29, 2009, President

---

[1] Cloud computing is a virtual infrastructure aimed to provide shared information and communication technology services, via a cloud, for many external users through use of the Internet.

[2] Shon Harris, *All-in-one CISSP Exam Guide* (New York: McGraw Hill, 2010), 7.

[3] Rutrel Yasin, "House panel questions cloud computing assumptions," Government Computer News, July 1, 2010, at: http://gcn.com/articles/2010/07/01/congress-hearings-on-cloud-computing.aspx (accessed September 10, 2010).

Obama named cyber security as a top economic and national security priority as a result of his 60-day review that called for securing information systems used by the government and the U.S. economy. Moreover, he stated,

> [P]rotecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.[4]

The analysis of threats and countermeasures in each of the ten domains of the CISSP CBK will provide lessons learned to ensure a secure implementation of cloud computing within the DoD.

C. PROBLEMS AND HYPOTHESIS

Secretary of Defense Robert Gates stated the U.S. is "under cyber attack virtually all the time, every day."[5] The DoD reported spending over $100 million from September 2008 to March 2009 on repairs to damage resulting from cyber attacks.[6] In 2008, the DoD removed 1,500 computers from the Pentagon's unclassified network due to a cyber attack, and in the fall of 2008 banned external removable media devices to prevent the spread of viruses.[7] Brigadier General John A. Davis, commander of the Joint Task Force for Global Network Operations, after a cyberspace conference in Omaha, Nebraska, stated that investments are necessary up front on computer countermeasures rather than later for repairs.[8]

---

4 Brian Krebs, "Obama: Cyber security is a National Security Priority," *The Washington Post*, May 29, 2009, at: http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html (accessed Jun 13, 2010).

5 CBS Interactive Staff, "DoD Gates: We're always under cyberattack," ZDNet, April 22, 2009, at: http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770 (accessed May 17, 2010).

6 Elinor Mills, "Pentagon Spends Over $100 million on cyberattack cleanup," CNET News, April 7, 2009, at: http://news.cnet.com/8301-1009_3-10214416-83.html (accessed May 17 , 2010).

7 Ibid.

8 Lolita C. Baldor, "Pentagon spends $100M to fix Cyber Attacks," Physorg.com, April 7, 2009, at: http://www.physorg.com/news158333019.html (accessed May 17, 2010).

DoD information security is so diverse that military services and components are challenged to focus their efforts. Sims and Gerber in their book "Transforming U.S. Intelligence," recommend the following areas be addressed:

> Decreasing the inherent vulnerabilities within our hardware and software; increasing the difficulty of an adversary introducing vulnerabilities into our systems through life-cycle approaches; increasing our ability to deeply evaluate critical components-design for evaluation; increasing the cost and uncertainty to an adversary attempting to exploit our vulnerabilities; increasing the probability of detecting a component (hardware or software) behaving badly (violating a security requirement); increasing the probability of attributing bad behavior to an adversary; increasing the consequences to the attacker for bad behavior.[9]

With the DoD's latest implementation of cloud computing in the past two years, security remains a major concern. The Cloud Security Alliance (CSA), in consultation with thirty commercial security experts, published a report on the top security threats with cloud computing. These threats included: nefarious personnel working for cloud computing providers, malicious attackers targeting providers, lack of security in interfaces or application programming interfaces (APIs), vulnerabilities in shared technology, data loss or leakage; and lastly, service hijacking.[10]

In April 2010, CSA published results from a survey on cyber security stating that seventy percent of 198 respondents from across the military and government are "concerned about [the] data security, privacy and integrity" of cloud computing.[11] Also, during the latest Cloud Computing Summit in Washington, D.C., May 2010, the main lesson was "caveat emptor," which means "buyers beware" in Latin.[12]

One of the main problems with cloud computing is that a customer, such as the DoD, places trust in the protection of data (for privacy and security) with an outside

---

[9] Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005),106–107.

[10] Barbara DePompa. "The Cloud's Standard Imperative," *Defense Systems: Knowledge Technologies and Net-Centric Warfare,* May 5, 2010, at: http://defensesystems.com/microsites/2010/cloud-computing/cloud-standards-imperative.aspx (accessed May 29, 2010). This hack took place 4 May 2010.

[11] Ibid.

[12] Ibid.

commercial vendor. Since data is on the cloud, the IT management team of the cloud controls the security and privacy settings. Moreover, providers often work with third-party venders, and it is difficult to guarantee how all these interweaved parties safeguard data.[13]

1. Cloud Vulnerability

There are several incidents that highlight the need for DoD diligence with security in its adoption of cloud computing. CIA are of major concern for cloud computing in consideration of a rogue hacker, data outages, and data loss.

a. Hacked

The U.S. Treasury was recently negatively affected when the Bureau of Engraving and Printing's (BEP's) website was forced offline because its cloud computing vender was attacked using malicious code.[14] Another recent malicious attack transpired when a hacker allegedly gained access to a Twitter employee's personal email and Google apps account.[15] As a result, 310 of Twitter's financial notes and documents were downloaded from Google's cloud application, and subsequently circulated around the Internet.

b. Outage

After routine maintenance, servers at Gmail malfunctioned and caused a 100 minute outage on September 1, 2009.[16] In reference to the recent outages by Google, Microsoft, and Amazon, Tim O'Brien, director of platform strategy at Microsoft, stated,

---

[13] Karthik Kumar and Yung-Hsiang Lu. "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?" *Computer*, Vol. 44, No. 4 (April 2010),1–14.

[14] DePompa, "The Cloud's Standard Imperative."

[15] John D. Sutter, "Twitter hack raises questions about cloud computing," *CNN.com*, July 16, 2009, at: http://www.cnn.com/2009/TECH/07/16/twitter.hack/index.html (accessed July 13, 2010).

[16] Ben Traynor, "More on Today's Gmail Issue," *The Official Gmail Blog*, 9 September 2009, at: http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html (accessed June 13, 2010).

"outages are just a reality…[e]ven if you do your due diligence, you still have to manage around these risks."[17]

c. Data Loss

When Microsoft's Danger subsidiary failed, T-Mobile Sidekick mobile phone users experienced not only an outage, but also lost data in their contacts, calendar, and address book.[18] Sidekick's cloud solution with Microsoft failed and cost both companies reliability points with customers.[19]

These incidents clearly highlight the vulnerability of placing trust in cloud computing. Cloud security experts today, such as Dr. Bret Michael of the Naval Postgraduate School, assert that, "[i]t is unclear whether the current set of [cloud] services is sufficiently secure and reliable for use in sensitive government environments."[20] Moreover, Michael states, "[t]he current architectural approaches, especially those concerning security, may not scale to the much larger cloud computing approaches."[21] Clearly, there is cause for concern.

2. Addressing the Vulnerability

According to Heather Wald, an assurance and resiliency consultant for the Department of Commerce, many government agencies are concerned about inherent risks in cloud computing, but are lured by a potentially "cheaper, easier, and more secure" solution.[22] With many potential benefits offered by cloud, the DoD should continue to seriously investigate and address the risks associated with securing this architecture.

---

[17] Traynor, "More on Today's Gmail Issue."

[18] Ina Fried, "Software outage casts cloud over Microsoft," *CNET News*, October 10, 2009, at: http://news.cnet.com/8301-13860_3-10372525-56.html (accessed June 14, 2010).

[19] Ibid.

[20] Bret Michael and George Dinolt, "Establishing Trust in Cloud Computing," *Information Assurance (IA) Newsletter*, Vol. 13, No. 2 (Spring 2010), 6.

[21] Ibid.

[22] Heather Wald, "Cloud Computing for the Federal Community," *Information Assurance Newsletter*, Vol. 13, No. 2 (Spring 2010), 10.

The purpose of this thesis is to identify countermeasures that will strengthen the security posture of cloud computing for the DoD. This is done by using the ten domains of the CISSP CBK as a framework for examining cloud security recommendations.

D. METHODS AND SOURCES

This thesis will include a historical analysis of threats and attacks against cloud computing, as well as countermeasures within the context of the ten domains of the CISSP CBK. The ten domains of the CISSP CBK provide a framework for the areas of research, along with a variety of text books, industry web sites (such as the U.S. Computer Emergency Response Team), professional journals and the most current articles from computer security publications.

E. OVERVIEW OF THESIS

Chapter I addressed the major research question of this thesis and why it is important. It also covered problems and hypothesis, and methods and sources. Chapter II reviews the literature in order to define cloud computing, stipulate pros and cons of cloud computing, describe the four types of cloud solutions and cloud service models, describe current instances of clouds in the DoD, justify and characterize the ten domains, and identify security advantages and challenges of cloud computing. Chapter III discusses the future of cloud computing in the federal government and the DoD. Chapter IV stipulates the inherent risk of using an external provider or even managing an internal cloud. Chapter V dissects the ten domains for threats and countermeasures as they apply to clouds. Chapter VI summarizes the findings.

II. LITERATURE REVIEW

A. WHAT IS CLOUD COMPUTING?

Cloud computing is an evolving paradigm with changing definitions, but for this research project, it is defined as a virtual infrastructure which provides shared information and communication technology services, via an internet "cloud," for "multiple external users" through use of the Internet or "large-scale private networks."[23] Cloud computing provides a computer user access to Information Technology (IT) services (i.e., applications, servers, data storage) without requiring an understanding of the technology or even ownership of the infrastructure.[24]

To comprehend cloud computing, an analogy to an electricity computing grid is useful. A power company maintains and owns the infrastructure, a distribution company disseminates the electricity, and the consumer merely uses the resources without ownership or operational responsibilities.[25] Similarly, a user's cloud computing access enables "shared resources, software, and information on-demand" on a fee-for-service basis.[26]

According to the National Institute of Standards and Technology (NIST), cloud computing exhibits several characteristics:[27]

- "On-demand self-service"—users can automatically request and obtain provisions of "server time and network storage."
- "Broad network access"—access to network is available through multiple platforms (i.e., cellular phones, laptops, and Personal Digital Assistants);

---

23 Joseph Katzman and Fred Donovan, "Head in the Clouds: DoD Turns to Cloud Computing," Defense Industry Daily. May 25, 2010, at: http://www.defenseindustrydaily.com/defense-cloud-computing-06387/ (accessed May 29, 2010).

24 Ibid.

25 Ibid.

26 Ibid.

27 Katzman and Donovan, "Head in the Clouds: DoD Turns to Cloud Computing."

- "Resource pooling"—the provider collocates resources (applications, memory, bandwidth, virtual machines) to service many users regardless of location.
- "Rapid elasticity"—resources are provided quickly (often automatically) and in a scalable manner (more is available and provided if more is needed and less is provided if less is needed).
- "Utility Computing"—the provider transparently meters, monitors, controls and documents service usage for billing.

B. PROS AND CONS TO CLOUD COMPUTING

The services within cloud computing contain a layered architecture of resources with many benefits. First, the IT network is managed by an external provider, and the customer does not need to maintain servers, train IT employees or even purchase software licenses.[28] This lowers monetary costs in personnel requirements/training, power, infrastructure maintenance, and storage space.[29] Cloud computing increases scalability (computer capability can grow in response to increases in customer demand), expediency in new service roll out, availability (a loss of one component will not disconnect all components), and mobility (the ability to telecommute).[30] Cloud computing increases the flexibility of organizations due to information sharing and collaboration (multi-tenancy).[31]

The services and architecture of cloud computing contain some areas of concern. Security implementations will require additional monetary resources to implement.[32] Turning data turned over to a third party cloud provider creates concerns with trust (privacy and security of data).[33] An increased geographic distance between users and

[28] Katzman and Donovan, "Head in the Clouds: DoD Turns to Cloud Computing."

[29] Heather Wald, "Cloud Computing for the Federal Community." *Information Assurance Newletter*, Vol. 13, No. 2 (Spring 2010), 14.

[30] Manish Pokharel and Jong Sou Park, "Cloud Computing: Future solution for e-Governance," *ACM*, 2009: 408–410.

[31] Katzman and Donovan, "Head in the Clouds: DoD Turns to Cloud Computing."

[32] Wald, "Cloud Computing for the Federal Community."

[33] Ibid., 14.

applications/data can introduce latency problems.[34] Service Level Agreements (SLAs) with providers are less robust than required for a company providing IT services. Governance and security standards in regard to cloud computing are currently lacking. Centralization of data presents security concerns, in addition to nefarious use of cloud computing architectures.

C. CLOUD COMPUTING DEPLOYMENT MODELS

There are four types of clouds that the DoD can potentially invest: public (external), private (internal), community (a subset of public/private), and hybrid (combination of any two or more above).

1. Public Cloud

A public cloud provides shared resources via a web application to many unrelated customers; the provider maintains the cloud.[35] Billing is based on a utility-type configuration. The Department of Navy Chief Information Officer stated, "Public clouds are not necessarily appropriate for Army or Navy information to be just sitting out there."[36]

Two benefits to a public cloud are that it is cost effective; and an external provider performs the security.[37] Two detractors to a public cloud solution include: client concerns about the level of security, and the difficulties with a provider showing securing compliance.[38]

---

[34] Frederic Paul, "Cloud Computing's Dirty Little Secret," Enterprise Efficiency, August 30, 2010, at: http://www.enterpriseefficiency.com/author.asp?section_id=898&doc_id=196259 (accessed October 2, 2010).

[35] Wald, "Cloud Computing for the Federal Community."

[36] Dorothy Ramienski, "DoD IT experts open up about cloud deployment," *Federal Executive Forum*, November 10, 2009, at: http://www.federalnewsradio.com/index.php?nid=35&sid=1808816 (accessed August 11, 2010).

[37] Wald, "Cloud Computing for the Federal Community."

[38] Ibid.

2. Private Cloud

A private cloud is built, managed, and directly controlled by the customer, and deemed the most secure type of cloud solution when correctly managed.[39] Another definition of a private cloud is a cloud infrastructure

> …operated solely for a single organization. It may be managed by the organization or a third party, and may exist on premises or off-premises.[40]

The private cloud is the preferred implementation for the DoD, as per Mr. Robert F. Lentz, Deputy Assistant Secretary of Defense, for Cyber, Identify and IA, in his speech to the House of Representatives on May 5, 2009.[41] Some of the benefits to a private cloud solution include, (1) it was deemed the "most secure model" based on a client implementing the solution in a secure manner; and (2) it is a "more efficient use of physical IT assets" when contrasted with a traditional data center.[42]

Some of the detractors to a private cloud solution include (1) loss of monetary efficiencies and savings gained from an outsourced cloud, (2) it cannot solve traditional data implementation difficulties, and (3) the burden of internal network management.[43]

3. Community Cloud

A community cloud provides service for many clients, and falls within the continuum of a public and private cloud, and therefore, could be managed by an organization or a third party on- or off-premises.[44] The tenants of this cloud type are related in mission.[45] Unlike public clouds, community clouds are designed to

---

[39] Wald, "Cloud Computing for the Federal Community."

[40] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" *Cloud Security Alliance*, December 2009, at: http://www.cloudsecurityalliance.org/guidance/csaguide.pdf (accessed August 3, 2010), 17.

[41] Robert F. Lentz, "Statement before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities,"

[42] Wald, "Cloud Computing for the Federal Community," 18.

[43] Ibid.

[44] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" 17.

[45] Wald, "Cloud Computing for the Federal Community."

accommodate customer desires and requirements (including governance). The Federal Chief Information Officer (CIO) announced the launch of apps.gov, a government community cloud, in conjunction with Google publicizing plans to build a community government cloud in compliance with government policies.[46]

Some of the benefits to a community cloud solution include (1) it is custom built, which means it can meld to comply with given standards; (2) it contains the economic efficiencies and advantages of a public cloud; and (3) the customer is only required to pay for services used.[47] One disadvantage to a community cloud solution is the potential for data leakage.[48]

4. Hybrid Cloud

> The hybrid cloud is composed of two or more cloud types, which are
>
> Bound by a standard or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds.[49]

The hybrid cloud manifests many of the pros and cons of its counterparts.[50]

5. Private Cloud Recommended by DoD

For the highest levels of security, organizations must incorporate a private cloud (although costs increase); some public clouds are currently in use by the DoD, where sensitivity of data (e.g., personal identifiable information) is not a concern.[51] The DoD is currently using public and private cloud solutions.

---

[46] Thomas Claburn, "*Google Plans Private Government Cloud*," Information Week Government, September 16, 2009, at: http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=220000732&pgno=1&queryText=&isPrev (accessed August 11, 2010).

[47] Wald, "Cloud Computing for the Federal Community."

[48] Ibid.

[49] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 17.

[50] Wald, "Cloud Computing for the Federal Community."

[51] Roger Halbheer, "*Moving to the Cloud in an Azure Sky: A security Review,"* Power point briefing, Microsoft Corporation, at: http://halbheer.info/security (accessed Aug 3, 2010).

Mr. Robert F. Lentz, Deputy Assistant Secretary of Defense, for Cyber, Identify and IA, stated, "For many DoD applications, the commercial cloud will be too risky, but a private cloud could bring many benefits."[52] Lentz also suggested that the DoD could reap financial gains by providing its own private cloud to members of the DoD.[53] He listed the benefits to capitalize upon as net-centricity, "scalable, on-demand computing, virtual monitoring, and provisioning," and widespread information sharing.[54]

D. CLOUD COMPUTING SERVICE MODELS

There are three types of cloud service models: Infrastructure, Platform and Software as a Service. The software layer builds upon platform, while platform builds upon infrastructure.[55]

1. Infrastructure as a Service (IaaS)

With this model, a customer rents physical facilities, connectivity, and hardware to deploy customer software, operating systems and applications; specific IaaS vendors include "Amazon EC2, GoGrid, and FlexiScale."[56] With IaaS, a customer is not required to manage/purchase servers and network infrastructure equipment, even though configuration management is still required. One disadvantage to IaaS is that bandwidth delays may occur with remote execution.[57]

2. Platform as a Service (PaaS)

This model enables a customer to rent a platform (hardware, storage, or virtual computers) to deploy its own specifically created applications; applications are then

---

[52] Robert F. Lentz, "Statement before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities," 18.

[53] Ibid., 19.

[54] Ibid., 18.

[55] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1."

[56] Wald, "Cloud Computing for the Federal Community."

[57] Mel Beckman, "Cloud Options that IT will Love," *An Interactive eBook: Cloud Computing*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

supported by the provider.[58] PaaS is middleware, which can include access/identity/authentication management; specific vendors of PaaS include "Force.com, Google, AppEngine and Coghead."[59] One specific beneficial use of PaaS is the development of standardized software programs.

3. Software as a Service (SaaS)

SaaS allows a customer to rent software applications provided over the Internet via a thin client/web browser (user does not own or control the infrastructure, servers, operating system, or storage); specific SaaS vendors include "Salesforce.com, GoogleApps, and Oracle on Demand."[60]

4. Security Tradeoffs between Service Models [61]

SaaS contains the highest integrated security functionality "with the least customer extensibility" since the provider bears a majority of responsibility for security.[62] PaaS allows developers to build applications, hence is "more extensible than SaaS;" customers are allowed more flexibility in adding security with the applications added, and developed.[63] IaaS enables vast extensibility, as the provider must protect the infrastructure; the customer is required to secure and manage "operating systems, applications and content."[64]

A customer is responsible for security and management where the provider's responsibility in the stack stops.[65] SaaS requires SLAs to stipulate responsibilities

---

[58] Bret Michael and George Dinolt, "Establishing Trust in Cloud Computing," *Information Assurance Newsletter*, Vol. 13, No. 2 (Spring 2010).

[59] Allan Carey, "Cloud Assurance Still Missing," *Information Assurance Newsletter*, Vol. 13, No. 1 (Winter 2010), 34.

[60] Ibid.

[61] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1."

[62] Ibid., 19.

[63] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1."

[64] Ibid.

[65] Ibid.

between the provider and customer, while PaaS and IaaS require customer system administration, even though a provider will secure the platform and infrastructure for availability.[66]

E. WHAT IS CURRENT IN THE DOD?

Currently in the DoD, there are four known implementations of cloud computing with many more starting up, including use of cloud in Afghanistan for biometric support.[67] These four implementations include (1) the Army's Experience Center (AEC), (2) Defense Information System Agency's (DISA's) Rapid Access Computing Environment (RACE); (3) Forge.mil; and, (4) the Air Force's Personnel Services Delivery Transformation (PSDT).[68]

1. Army Experience Center (AEC)

A successor to the Army Recruiting Information Support System, the AEC cloud solution is in pilot mode as a public/community cloud providing SaaS,[69] as of 2008. The AEC uses Salesforce.com as a customer relationship management tool to track recruits by integrating email, Twitter, and Facebook for dynamic social interactions.[70] Cloud computing increased the speed of response times from recruiters.[71]

2. Rapid Access Computing Environment (RACE)

DISA began using RACE, a private/community DoD cloud providing PaaS, in 2008. Starting in October 2009, RACE offered DoD users a "self-service provision

---

[66] Ibid., 19.

[67] Ellen Messmer, "US military takes cloud computing to Afghanistan," September 23, 2010, Network World, at: http://www.networkworld.com/news/2010/092310-cloud-computing-afghanistan.html?page=1 (accessed October 1, 2010).

[68] Vivek Kundra, *State of Public Sector Cloud Computing*, Washington, D.C.: Federal Chief Information Officer, May 20, 2010.

[69] Vivek Kundra, "Public Sector Cloud Computing Case Study: Army Experience Center," *CIO.GOV Website*, June 8, 2010, at: http://cio.gov/pages.cfm/page/Public-Sector-Cloud-Computing-Case-Study-Army-Experience-Center (accessed October 27, 2010).

[70] Kundra, "Public Sector Cloud Computing Case Study: Army Experience Center."

[71] Ibid.

operating environment within the highly secured Defense Enterprise Computing Center's production environment."[72] Users can customize and purchase test and computing platforms quickly and cheaply.[73] DISA implemented "pre-established IA controls" in testing and production environments,[74] and is in the process of integrating a "host-tenant accreditation model" to ensure compliance with the DoD IA Certification and Accreditation Process (DIACAP).[75]

3. Forge.mil

Forge.mil is a private/community DoD cloud providing SaaS,[76] and specifically used by DISA to create, test and deploy software and other systems.[77] Forge.mil saves resources through "economies of scale, ubiquitous delivery…and cross collaboration."[78] DISA uses a cloud provider platform from CollabNet,[79] which services 5,000 users across 300 projects; this solution gloats $200 to $500,000 in savings per project, and an additional $15 million in "cost avoidance by utilizing an open source philosophy" of collaborative development and software reuse.[80] Since forge.mil is an open source solution mixed with cloud computing, other benefits include version control, traceability,

72 Defense Market, "DoD Embraces Cloud Computing" Defense Market Research and Analysis, October 29, 2010, at: http://www.defensemarket.com/?p=67 (accessed May 31, 2010), p. 1.

73 Kundra, *State of Public Sector Cloud Computing*.

74 Ibid.

75 Christopher Perry, "Security for Cloud Computing," Department of the Navy Chief Information Officer Website, May 18, 2010, at: http://www.doncio.navy.mil/ContentView.aspx?ID=1744 (accessed August 27, 2010).

76 This was found under frequently asked questions of the forge.mil website: http://www.forge.mil/Faqs.html#faqs1 (accessed October 27, 2010).

77 Kundra, *State of Public Sector Cloud Computing*, 19.

78 Ibid.

79 This was found under frequently asked questions of the forge.mil website: http://www.forge.mil/Faqs.html#faqs1 (accessed October 27, 2010).

80 Ibid.

shortened time-to-market, and collaboration.[81] This solution is utilized by the Army, Navy, Air Force, Marine Corps, and the Joint Chiefs of Staff.[82]

4. Personnel Services Delivery Transformation (PSDT)

The Air Force Personnel Center (AFPC) implemented a private/community DoD SaaS solution, provided by RightNow,[83] to increase efficiencies in customer service, "knowledge management and case tracking."[84] With this SaaS solution, AFPC efficiently completed a manpower reduction initiative, which saved $4 million annually while increasing customer service/engagement by 70 percent.[85]

F. JUSTIFICATION FOR THE TEN DOMAINS

Historically, the information system security profession did not contain structure, objectives or discipline.[86] In the 1980s, members of the profession decided to implement structure and provide evidence of their competence through qualifications.[87] Professional credibility blossomed to fruition in mid-1989 when the International Information Systems Security Certification Consortium, Inc., (ISC)2, was formed to develop certification programs for information security professionals.[88] The consortium adopted "an information systems security CBK" with ten domains because of the "broad and diversified" nature of technology within business.[89] The ten domains stemmed from

---

[81] This was found under frequently asked questions of the forge.mil website: http://www.forge.mil/Faqs.html#faqs1 (accessed October 27, 2010).

[82] Ibid.

[83] The name of the SaaS provider was located at this source: Bozeman, Mont., "U.S. Air Force Personnel Center Works with RightNow to Tap into Cloud," RightNow.com, May 12, 2009, at: http://www.rightnow.com/crm-news-7434.php (accessed October 27, 2010).

[84] Kundra, *State of Public Sector Cloud Computing*, 19.

[85] Ibid.

[86] Harris, *All-in-one CISSP Exam Guide*.

[87] Ibid.

[88] W. Hord Tipton. "(ISC)2 Website," *Information Systems Security Certification Consortium*, at: http://www.(ISC)2.org/aboutus/default.aspx (accessed May 27, 2010).

[89] Harris, *All-in-one CISSP Exam Guide*, 8.

three tenets of information security: CIA. These domains provide a framework for information security qualifications and credentials in the field.

In order to comply with the Federal Information Security Management Act (FISMA), on May 15, 2008, the DoD established a policy requiring military and civilian personnel to obtain commercial IA certifications from (ISC)2 within six months of filling an IA billet.[90] Depending on whether the DoD employee is a manager or technician determines the type of certification required. A technician, level III, and a manager, levels II and III, are required to become CISSPs.[91] Along with industry, the DoD mandated this level of intense training, inclusive of the ten domains, as a necessity for securing its information infrastructure.

A framework of CIA and a standard within industry and the DoD, the ten domains of the CISSP CBK provide a credentialed paradigm for research of threats and countermeasures necessary for strengthening the information security posture of cloud computing within the DoD.

G. DESCRIPTIONS OF THE TEN DOMAINS

1. Access Control

Access control encompasses all mechanisms which allow managers to direct and restrain not only content, but user behavior/use of a system.[92] Managers control subject (person, machine, or processes) access to objects or resources in a system, as well as the permissions with those resources, i.e., read, write, execute.[93] Loopholes in any of these mechanisms expose systems to exploitation. These attacks can take place by insiders or outsiders. Once access is obtained to a network, an intruder or attacker can access internal IT infrastructures.

---

[90] DoD 8570.01-M, "*IA Workforce Improvement Program*," May 15, 2008, at: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed May 27, 2010).

[91] Ibid.

[92] Harold F. Tipton, *Official (ISC)2 Guide to the CISSP CBK*, (Boca Raton: Taylor and Francis Group, LLC, 2010), xii.

[93] DoD 8570.01-M, "*IA Workforce Improvement Program*," May 15, 2008, at: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed May 27, 2010).

2. Telecommunications and Network Security

The telecommunications and network security domain includes

> the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communication networks and media.[94]

Other arenas of this domain include voice and data communications for local and wide area networks, as well as remote connections to the network.[95] More areas include firewalls, routers, internet, extranet and internet, and TCP/IP.[96] This domain specializes in preventing, detecting and correcting communications for secure and available services.[97]

3. Information Security Governance and Risk Management

This domain examines policy, data classification, risk assessment, and personnel security and training.[98] Governance involves implementation of administrative, technical and physical controls that secure information systems. These three areas of governance include: (1) administrative—policy & procedures, risk management, screening employees, awareness training, and change control; (2) technical—access control mechanisms, resource management, configuration management; and (3) physical—facility access, facility perimeter protection, intrusion monitoring & environmental controls.[99]

Information risk management involves identification and assessment of risks, reducing those risks to a level that is acceptable, and then implementing countermeasures

---

[94] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, xv.

[95] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

[96] Ibid.

[97] Ibid.

[98] Harris, *All-in-one CISSP Exam Guide*, 7.

[99] Ibid., 49.

to maintain that level.[100] Risks can involve physical damage, human interaction, equipment malfunction, inside and outside attack, data misuse or loss, and errors within applications.[101]

4. Application Security

This domain explores effective development and measurement of operating system and application security components.[102] Within application security, web security addresses a myriad of attacks, such as vandalism, denial of service, financial fraud, privileged access, and theft of transaction information or intellectual property.[103] Other threats to web environments include information gathering, administrative interfaces, authentication and access control, configuration management, input validation, parameter validation, and session management.[104] Safeguards for mitigating these risks include quality assurance programs, web application firewalls, intrusion prevention systems, and SYN proxies on the firewall.[105]

5. Cryptography

Cryptography includes methods of disguising and authenticating information using technologies such as public key infrastructure, hashes, and symmetric and asymmetric encryption algorithms.[106] Cryptography is a primary means to provide confidentiality of information to deny an unauthorized user access. Moreover, use of a digital signature can provide authentication of a sender as well as non-repudiation, which means the sender cannot deny sending the message. Hashing can provide an integrity check for information when passing critical information between entities.

---

[100] Harris, *All-in-one CISSP Exam Guide*, 73.

[101] Ibid.

[102] Ibid., 7.

[103] Ibid.

[104] Harris, *All-in-one CISSP Exam Guide*,1003.

[105] Ibid., 1002–1003.

[106] Ibid., 7.

6. Security Architecture and Design

This domain examines how to design and build secure systems. Some of the main issues in securing an information system include use of protection rings, layering and data hiding to provide integrity and confidentiality.[107] Additionally, security models and policy are necessary to ensure proper countermeasures are in place, as well as certification and accreditation of systems. Several threats of concern in this domain include maintenance hooks, time-of-check/time-of-use attacks, and buffer overflows, which all have corresponding countermeasures such as proper programming, nonces and time stamps, and parameter checking.

7. Operational Security (OPSEC)

OPSEC is used in identification of "controls over hardware, media, and the operators with access privileges to any of these resources," which is inclusive of auditing and monitoring of processes involved in security reporting.[108] OPSEC includes all activities needed to maintain "network, computer systems, applications and environments up and running in a secure and protected manner."[109] Several operational security attacks include fingerprinting, packet sniffing, social engineering, and man-in-the-middle, while countermeasures include encryption and user training.[110]

8. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

BCP and DRP examine methods to ensure continuous operations as well as system recovery during disruption. The steps to developing a BCP include project initiation, business impact analysis, recovery strategy, design and development,

---

[107] Harris, *All-in-one CISSP Exam Guide*, 314.

[108] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, xiv.

[109] Harris, *All-in-one CISSP Exam Guide*, 1049.

[110] Harris, *All-in-one CISSP Exam Guide.*

implementation, testing and continual maintenance.[111] A security policy and program must encompass a BCP. Effective maintenance of data backups is also integral to this domain.

9. Legal Regulations, Compliance, and Investigation

Legal regulations, compliance, and investigation encompass laws and crimes involving information systems. There is a distinction between computer-targeted and computer-assisted crimes. In computer-assisted, the computer is just a tool to help carry out a crime, while in computer targeted, the computer is actually the victim of an attack.[112] The main issues in this domain are jurisdiction, how to present evidence to a judge, and the fact that laws do not keep up with technology. Some attacks within this domain include salami, data diddling, excessive privileges, password sniffing, IP spoofing, dumpster diving, emanations capturing, and wiretapping.[113]

10. Physical and Environmental Security

Physical and environmental security examines protection of facilities, personnel and information systems through environment, entry methods and safety.[114] Specific areas of interest in this domain include crime prevention through environmental design, power, ventilation and fire considerations, and perimeter security implementations.[115]

H. SECURITY ADVANTAGES TO CLOUD COMPUTING

The security advantages of cloud computing are prolific:

---

[111] Harris, *All-in-one CISSP Exam Guide*, 780.

[112] Ibid., 847.

[113] Ibid., 903–906.

[114] Harris, *All-in-one CISSP Exam Guide*, 7.

[115] Ibid.

- *Security automation*. The homogeneity of a cloud environment facilitates automation in auditing/testing/security/data retention,[116] which increases the speed of request, change, release, configuration, compliance, capacity, and patch management.[117]

- *Centralization of data.* Centralization of data facilitates "patch[ing], upgrad[ing], monitor[ing] and encrypt[ing]" data.[118] It also decreases the area needed to collocate or provide physical security because the perimeter is smaller.

- *Mirroring assists in data recovery.* Replicated content or redundancy, as well as multiple storage sites, provides an excellent source for both disaster recovery and business continuity controls.[119]

- *Data provisions by zone*. Zones create partitions that block information spillage.[120] These provisions also can prevent reverberations during a denial of service attack.

- *Encryption.* "Encryption of data at rest and in transit" protects confidentiality of a user's data.[121]

- *Buying security in bulk.* Every type of security measure, (i.e., filtering, authentication, access control measures, federated identity management)

---

[116] Lee Badger and Tim Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing," *NIST Computer Security Division Briefing*, May 20, 2010, at: http://www.slideshare.net/kvjacksn/nist-cloud-computingforumbadgergrance (accessed November 24, 2010).

[117] Ben Newton, "Building Private and Community Clouds for the DoD," Defense Systems, September 23, 2010, at: http://defensesystems.com/Articles/2010/09/02/Industry-Perspective-Automating-the-Cloud.aspx?Page=2 (accessed October 1, 2010).

[118] Naxal Watch, "U.S.: DoD Advances Cloud Computing Usage," Intellibriefs, January 12, 2010, at: http://intellibriefs.blogspot.com/2010/01/us-dod-advances-cloud-computing-usage.html (accessed October 1, 2010).

[119] Badger and Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing."

[120] Badger and Grance, "Standards Acceleration to Jumpstart Adoption of Cloud Computing."

[121] Ibid.

when implemented on a larger scale, is cheaper, in that "the same amount of investment buys better protection."[122]

- *Audit and forensic investigation*. With IaaS, customers can create live virtual images, and image components, in order to conduct investigations.[123]
- *Ubiquity or infinite availability of data*. Cloud Computing provides dynamic resource availability and portability, which could prove useful for military operations if properly secured.[124]

I. SECURITY CHALLENGES WITH CLOUD COMPUTING

There are many security challenges with cloud computing. Some of the recognized challenges or risks include:

- *External reliance for securing data*. Reliance on an external provider for security (physical, logical, personnel and security controls) can add risk to the CIA of customer data.[125] An alarming 22 out of 24 major federal agencies reported being "concerned or very concerned" about general security risks with cloud computing.[126] This dependence on an external provider could result in lost data or an inability to transfer data, and requires the customer to monitor and examine security controls.[127] In a survey conducted by the U.S. Government Accountability Office (GAO), major agencies reported concerns about "ineffective or non-compliant service provider security controls," lack of security control in delegation to third parties, and lack of comprehensive security investigations when hiring provider personnel.[128] A customer should obtain information about

---

[122] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," *European Network and Information Security Agency*, November 2009, at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (accessed August 6, 2010), 17–20.

[123] Ibid., 18.

124 Naxal Watch, "U.S.: DoD Advances Cloud Computing Usage," *Intellibriefs*, January 12, 2010, at: http://intellibriefs.blogspot.com/2010/01/us-dod-advances-cloud-computing-usage.html (accessed October 1, 2010).

[125] Gregory C. Wilshusen, *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing*, July 1, 2010, at: http://www.gao.gov/new.items/d10513.pdf (accessed October 7, 2010).

[126] Ibid.

[127] Wilshusen, *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.*

[128] Ibid., 3–4.

hiring practices as well as oversight of administrative privileges and access.[129]

- *Scarce federal security guidance/procurement strategy*. Comprehensive security guidance in the federal government is yet to be available.[130] Even though the Federal CIO created a cloud computing executive steering group, guidance is pending. Also, NIST is still working on specific cloud standards for security guidance.[131] In a report released July 1, 2010, the U.S. GAO recommended that the Office of Management and Budget, the General Services Administration, and the Department of Commerce develop a strategy for integrating security into the procurement process for cloud computing services.[132]
- *Regulation compliance of cloud providers.* Traditional IT service providers are subject to audits and accreditation, therefore cloud providers should not be exempt.[133]
- *Identity management problems*. Improper identity management could compromise authentication or authorization to access data.[134]
- *Confusion with responsibilities*. There is often confusion over responsibilities regarding incident response, response to an audit finding or forensic investigation.[135] Agencies voiced challenges with defining responsibilities and roles of vendor verses customer in cloud computing implementations.[136]
- *General cloud security issues*. Some of these challenges include: knowing the physical location of data and the provider's adherence to local privacy

---

[129] Jon Brodkin, "Gartner: Seven cloud computing security risks," Infoworld, July 2, 2008, at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0 (accessed November 6, 2010).

[130] During the time this thesis was written, federal guidance was provided and can be found at this link: http://www.govinfosecurity.com/articles.php?art_id=3063 (this link is also reference in the information security governance and risk management section of this thesis.

[131] Wilshusen, *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.*

[132] Ibid., Introduction page.

[133] Jon Brodkin, "Gartner: Seven cloud computing security risks," Infoworld, July 2, 2008, at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0 (accessed November 6, 2010).

[134] Wilshusen, *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.*

[135] Wilshusen, *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.*

[136] Ibid., Introduction page.

laws;[137] the inability to access proprietary security implementations for testing; lack of accountability with system administrators; isolation management of data and permissions in a multi-tenant environment (e.g., use of encryption);[138] ensuring a storage controller or hypervisor does not present a single point of failure; DRP and continuity of operations (what happens to data in case of disaster, and how long does data restoration take?);[139] properly using SLAs to securely implement an external cloud provider's services (e.g., investigative support despite logging co-location);[140] and long-term viability[141] (CIA of data despite cloud company going out of business or transferring service to another provider).[142]

- *Elasticity challenges*. The dynamic nature of elasticity (through use of virtualization) brings unique security challenges:[143]

- *Traversal vulnerability*. The traversal vulnerability allows an individual to traverse from one VM to another if managed by the same hypervisor. This vulnerability requires protective administrative separation between customers. This is a major challenge to providers since the premise of their financial gains rests on "shared administrative management systems (i.e., hypervisors) across multiple virtual customer environments" (p. 3). (note: solution is stringent/granular access controls).

- *Encryption*. The traversal vulnerability could easily negate any front end encryption for data-at-rest within a virtual milieu. (note: solution could entail research into a provider's means for encryption in a shared environment).

- *Configuration/change management*. A problem with elasticity is enforcing strict and proper configuration/change management at the PaaS/IaaS level. (note: solution is stringent/granular access controls, i.e., which actions are allowed, as well as when and under what conditions these actions are taken; mechanisms for enforcing change policies are also needed).

---

[137] Brodkin, "Gartner: Seven cloud computing security risks."

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] Ibid.

[142] Peter Mell and Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm," National Institute for Standards and Technology, IT Laboratory, October 7, 2009, at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010), slide 45.

[143] Dustin Owens, "Securing Elasticity in the Cloud," Association for Computing Machinery, May 6, 2010, at: http://queue.acm.org/detail.cfm?id=1794516 (accessed September 10, 2010), 1.

- *Integrity within zones*. The challenge of protecting integrity within different zones of test, development and production environments.
- *Management control.* Control of management authorizations of expanding services.

Specific DoD cloud computing security challenges. Many of the above challenges will apply to the DoD, but some security challenges are slightly unique. The DoD might experience cyber attacks as a result of wartime missions, such as a tactical cloud solution which becomes subject to attack during a mission.[144] The DoD uses many different classification levels, under different authorities, which may present challenges with "sanitization/purging of local storage, data labeling, privilege-based access control…, [and] tailoring common operating pictures" to these different levels of access or privilege.[145] Finally, certification and accreditation is challenging in a provisioned infrastructure.[146] While the DoD may have a few unique challenges, many of these might be similar to what commercial organizations face in protecting their sensitive data for financial/proprietary verses wartime incentives.

[144] Chris Kubic, "DoD Cloud Computing Security Challenges," Briefing by Chief Architect, Information Assurance Architecture and Systems Security Engineering Group, National Security Agency, at: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf (November 6, 2010).

[145] Ibid., slide 7.

[146] Ibid.

III. THE FUTURE OF CLOUD

The issues in this section touch on cloud computing revenue projections, future uses and implementations, and the way ahead for the federal government and the DoD. As this thesis is about securing the cloud computing infrastructure, the future direction of this technology provides a framework from which to operate and orient.

Bountiful Revenues. Cloud adoption among enterprises is accelerating in an explosive manner as IT providers try to capitalize on cloud services.[147] IT expert, Gartner, Inc., forecasted revenue for worldwide cloud services as $68.3 billion this year, with a 16.6 percent increase from 2009.[148] By 2014, cloud computing is projected to reach revenues of $148.8 billion.[149] In the next five years, an estimated $112 billion will be spent on SaaS, PaaS and IaaS collectively.[150] Due to recessionary concerns, cloud computing will gain even more momentum as enterprises cut costs and attempt to create efficiencies with business processes.[151] In 2009, the U.S. share of cloud services was 60 percent, but is projected to dilute as other nations begin adoption for a share in the market; predictions include: Western Europe—23.8 percent of market (2010), Japan—10 percent of market (2010), U.K—29 percent of market (2014), and Japan—12 percent (2014).[152]

---

147 Christy Pettey and Ben Tudor, "Gartner Says Worldwide Cloud Services Market to Surpass $68B in 2010," *Gartner Newsroom*, June 22, 2010, at: http://www.gartner.com/it/page.jsp?id=1389313 (accessed October 23, 2010). Pettey is referring to the following cited report: Ben Pring, Robert H. Borwn, Lydia Leong, Adam W. Couture, Fabrizio Biscotti, Benoit J. Lheureux, Andrew Frank, Jeffrey Roster, Susan Cournoyer, and Venecia K. Liu, "Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014," June 2, 2010, Gartner, Inc, at: http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1378513 (accessed October 23, 2010).

148 Ibid.

149 Ibid.

150 Ibid.

151 Ibid.

152 Ibid.

Future Uses. Some researchers cite cloud computing as the future of electronic governance through a green and resource efficient IT solution.[153] Currently, the largest users of cloud exist in the finance and manufacturing industries, yet communications and IT will further leverage cloud computing, along with the public sector.[154]

What will Cloud look like in the future? The director of Microsoft's new research group, Cloud Computing Futures, predicted that future cloud infrastructures will contain seamless software upgrade/install without user interference, transparency between desktop and cloud environments, increases in power efficiencies, and more "resilient, adaptive, and reliable" software.[155] Enterprises such as Microsoft or other IT businesses will most likely use cloud services in combination with current services.[156]

The way ahead with security concerns for the federal government. While enterprise interest in cloud is increasing, security concerns still exist. Many enterprises are concerned about availability of service, and whether or not a vendor is viable and mature.[157] The Federal CIO stated, "To do more with less, we need game-changing technologies. Cloud computing is one such technology."[158] The Federal CIO also cautioned that the cloud should not be viewed as a financial "panacea" since security, operability and privacy concerns still exist.[159] Rep. Edolphus Towns, D-N.Y., provided his input about the federal future of cloud, "Government-wide implementation of cloud computing will be a decade-long journey;" he also voiced hopes that the federal

---

[153] Manish Pokharel and Jong Sou Park, "Cloud Computing: Future Solution for e-Governance," *ACM International Conference Proceeding Series*, Vol. 322, (New York: ACM, 2010), 409–410.

[154] Ibid.

[155] Rob Knies, "Peering into Future of Cloud Computing," *Microsoft Research*, February 24, 2009, at: http://research.microsoft.com/en-us/news/features/ccf-022409.aspx (accessed October 23, 2010), 1.

[156] Pettey and Tudor, "Gartner Says Worldwide Cloud Services Market to Surpass $68B in 2010."

[157] Ibid.

[158] John K. Higgins, "Uncle Sam Wants the Cloud, Part 1," *E-Commerce Times*, September 29, 2010, at: http://www.ecommercetimes.com/story/70924.html (accessed October 24, 2010), 1.

[159] Ibid.

government's launch to cloud computing is well thought out, that the benefits and risks are fully examined, and that there are comprehensive plans in place to ensure that we do this the right way, the first time.[160]

The federal government's first evident step toward a comprehensive plan was posed November 2, 2010, in a draft report, "Proposed Security Assessment and Authorization for U.S. Government Cloud Computing," which combined efforts by NIST, GSA, and the Information Security and Identity Management Committee (ISIMC), state/local governments, private sector.161 Inside the report was a petition for comments via www.fedRAMP.gov website through December 2, 2010. Clearly, the federal government via their CIO Vivek Kundra, is making monumental efforts toward securing the cloud.

The way ahead for The DoD. The DoD will capitalize on cloud computing as it already established RACE, trooptube.tv (a morale solution for troops and families),[162] and cloud-based biometric services in Afghanistan. More integrated projects are projected, and currently on the brink. These cloud projects will require creativity and collaboration with industry and other government organizations to bring to full fruition.

U.S. Army. One project in development by the U.S. Army is use of DISA services to consolidate disparate email systems into one centralized enterprise system with one help desk and one shared enterprise email service.[163] The Army CIO projects this effort will save over $100 million annually by bringing costs from $100 dollars to $40 dollars per user.[164] Other efficiencies will be gained by standardization and elimination of duplicated efforts. Inside this project, the Army CIO office is projected to move to the

160 Higgins, "Uncle Sam Wants the Cloud, Part 1."

161 Eric Chabrow, "White House Issues Secure Cloud Computing Guidance: FedRAMP Requirements aimed to easy cloud computing adoption," Government Information Security Articles, November 2, 2010, at: http://www.govinfosecurity.com/articles.php?art_id=3063 (accessed November 6, 2010).

162 Kubic, "DoD Cloud Computing Security Challenges."

163 J. Nicholas Hoover, "Army Consolidates Email Under DISA Cloud," Information Week Government, October 26, 2010, at: http://www.informationweek.com/news/government/enterprise-apps/showArticle.jhtml?articleID=227900731&queryText=cloud%20security (accessed October 31, 2010).

164 Hoover, "Army Consolidates Email Under DISA Cloud."

cloud in January 2011, the Army HQs by February 2011, and the rest of Army (1.4 million common access card holders) by October 2011.[165] Following the effort with the Army, the DoD has potential plans to migrate European, Transportation and Africa Commands, along with the rest of the services in the DoD, to this centralized email system.[166] The one central help desk will have a 1800 toll free phone number. Along with email plans, DISA is talking with Army CIO about plans to provide an enterprise Sharepoint solution.[167] One last concurrent/ongoing Army effort is a pilot project with 300 Army personnel using Google Apps; the pilot is being used to decipher the benefits of cloud computing for email in the DoD.[168]

U.S. Air Force. In February 2010, the Air Force awarded a contract to IBM for development of a cloud solution that introduces "advanced cyber security and analytic technologies" for protecting sensitive data.[169] The security effort, when reaching fruition, will impact Air Force network security across nine major commands, and 100 bases in support of 700,000 Air Force active duty personnel.[170] According to Lieutenant General William Lord, CIO and Chief, Warfighting Integration,

> Our goal is to demonstrate how cloud computing can be a tool to enable our Air Force to manage, monitor and secure the information flowing through our network. We examined the expertise of IBM's commercial performance in cloud computing and asked them to develop an architecture that could lead to improved performance within the Air Force environment to improve all operational, analytical and security capabilities.[171]

---

[165] Hoover, "Army Consolidates Email Under DISA Cloud."

[166] Ibid.

[167] Ibid.

[168] Ibid.

[169] Theo Chrisholm, "U.S. Air Force Selects IBM to Design and Demonstrate Mission-oriented Cloud Architecture for Cyber Security," *IBM Press Room*, February 4, 2010, at: http://www-03.ibm.com/press/us/en/pressrelease/29326.wss#release (accessed November 1, 2010), 1.

[170] Ibid.

[171] Ibid.

U.S. Navy.[172] In April of 2009, Rob Carey, the Navy CIO, suggested cloud computing be integrated into NGEN[173] and CANES[174]. He also proposed "grey clouds" on each ship. Currently, tentative moves by the Navy are in effect: San Diego State University is using a Google cloud platform (InRelief.org) to facilitate collaboration of diverse organizations responding to disasters. Carey sees garrison units as primary targets for cloud integration efforts over ships, due to the unique nature of ships at sea. Yet, during Trident Warrior,[175] Amazon Elastic Compute Cloud's IaaS was effective in connecting DoD applications and meeting mission storage requirements in support of operations. The implications could be that cloud services could assist Navy mission needs. Moreover, the Naval Air Warfare Center Weapons Division's Geophysics Branch, China Lake, California, signed a contract to use cloud services for weather forecasting, which could also take root if fruitful in execution.

Future DoD uses of cloud computing. Some proposed projects in the DoD include using cloud computing internally (private cloud) for "large-scale planning, execution and reporting of program test and evaluation" workflow processes within the U.S. Army.[176] Other uses could include logistical procurement, and intelligence collection and distribution ("storage/processing of tactical Intelligence, Surveillance, Reconnaissance (ISR) feeds").[177] Cloud computing could integrate with any solution for collaboration or interoperability of many users (i.e., ISR). It could be used for data center/system management, system auditing, monitoring/reporting, deployable operations

---

[172] Kevin Jackson, "CANES and the cloud," Military Information Technology, December 2009, at: http://www.military-information-technology.com/mit-archives/219-mit-2009-volume-13-issue-11/2353-canes-and-the-cloud.html (accessed November 6, 2010), Vol. 13, Issue 11.

[173] Next Generation Enterprise Network

[174] The Consolidated Afloat Network Enterprise System (CANES) is a term used to describe a part of the Navy's future IT strategy; through use of virtualization, CANES will reduce a ship's physical IT infrastructure.

[175] Trident Warrior is an annual Navy exercise for training personnel, and experimenting with maritime technologies.

[176] Jason S. Bolin, *Use Case Analysis for Adopting Cloud Computing in Army Test and Evaluation*, Naval Postgraduate School Master's Thesis, September 2010, at: http://edocs.nps.edu/npspubs/scholarly/theses/2010/Sep/10Sep_Bolin.pdf (accessed October 24, 2010).

[177] Kubic, "DoD Cloud Computing Security Challenges," slide 3.

overseas (e.g., for battlespace awareness to track personnel, missions, equipment; "simulation and visualization" for "mission planning and training"), and "cyber network defense."[178] Other uses of cloud services could include social networking, "data tagging, researching and indexing," and tactical environmental applications.[179] Further creative uses could be deciphered by using an OpenCrowd Taxonomy diagram that outlines service offerings by different companies (note: researcher is not advocating use of any particular provider).[180]

DoD is likely to continue to pursue cloud computing, especially given that President Obama has encouraged its use, specifically where efficiencies could be gained.

[178] Kubic, "DoD Cloud Computing Security Challenges," slide 3.

[179] Bolin, *Use Case Analysis for Adopting Cloud Computing in Army Test and Evaluation*, 115.

[180] Brunette and Mogull, "*Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1*," 20.

V. DISSECTING THE TEN DOMAINS

A. INTRODUCTION: INHERENT RISK WITH EXTERNAL PROVIDERS

The fundamental premise of cloud computing is to outsource an IT infrastructure from an internally (on-site) managed network operation to an external (off-site) network operation.[181] With this is in mind, four types of clouds (public, private, community, and hybrid) will dictate different security and implementation considerations. With external cloud services (public, community and hybrid clouds), the DoD must meticulously scrutinize the level of security. With a private cloud, the DoD can manage and police security for its own information systems.

The following discusses cloud threats and countermeasures relative to each of the ten domains. For the purposes of this research, the analysis of threats and recommendations/countermeasures will apply to both internal (private) and external (public) cloud implementations.

1. Access Control

Access controls are "security features that control how users and systems communicate and interact."[182] When a user is prompted for a user ID and password, this is considered an access control. A DoD cloud will require security mechanisms to preclude a cloud provider or external entity from pilfering through sensitive data.[183] Threats to access control in cloud computing include frictionless registration processes, account hijacking, generic authentication attacks, and insecure identity and access management. These threats and associated countermeasures are discussed.

---

[181] Russell Kay, "Quick Study: Cloud Computing," *An Interactive eBook: Cloud Computing*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

[182] Harris, *All-in-one CISSP Exam Guide* (New York: McGraw Hill, 2008), 155.

[183] Scott Paquette, Paul T. Jaeger, and Susan C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, Vol. 27, Issue 3 (July 2010).

Frictionless registration processes. Frictionless registration refers to the ease of an individual gaining access to a cloud without credentials or authorized access. The Top Cloud Threat report, published by the CSA in May 2010, warns that "frictionless" registration processes can enable anyone with a credit card access to a cloud; this in turn could open the cloud to malicious activities, i.e., spamming and propagating malicious code in an anonymous manner.[184]

Account hijacking. Attack methods to hijack an account include "phishing, fraud, and exploitation of software vulnerabilities."[185] Once an account is hijacked, the attacker can eavesdrop on a user, manipulate their data, and redirect information surreptitiously.[186] Recently, at a Black Hat Security Conference in July 2009, two researchers presented findings depicting how an attacker can "masquerade as any website [to]… trick a computer user into [disclosing]…sensitive communications."[187] If masquerading is used to mimic a cloud log in screen, a malicious attacker could gain a user's password and access to the account and associated data.

Generic authentication attacks.[188] Cloud computing authentication mechanisms are vulnerable to attack.[189] Potentially vulnerable authentication data (unless fortified with encryption) include: "user identities, passwords, biometric information, [and user] access capabilities."[190]

---

184 Dan Hubbard and Michael Sutton, "Top Threats to Cloud Computing, V1.0," *Cloud Security Alliance*, March 2010, at: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (accessed July 20, 2010).

185 Ibid.

186 Ibid.

187 Kim Zetter, "Vulnerabilities Allow Attacker to Impersonate Any Website," *Wired.com*, July 29, 2009, at: http://www.wired.com/threatlevel/2009/07/kaminsky/ (accessed July 23, 2010), 1.

188Michael Gregg, "Ten Security Concerns for Cloud Computing," *Global Knowledge Training, LLC: Expert Reference Series of White Papers*, 2010, at: http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_VI_10SecurityConcernsCloudComputing.pdf (accessed July 31, 2010).

189 Gregg, "Ten Security Concerns for Cloud Computing."

190 Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 28.

Countermeasures. Countermeasures to the preceding access control threats include: user training and awareness, using a multifactor authentication/registration process (two or more authentication methods of what a user has/is/knows), disallowing shared account credentials, proactively monitoring for unauthorized activities, not storing secret data on the cloud, and lastly, encryption of data in the cloud as well as authentication data.[191] Every single interaction in a cloud computing environment should be authorized and authenticated.[192]

Insecure overarching identity and access management problems. Challenges and corresponding recommendations with identity and access management are summarized below.[193]

- *Identity provisioning*. Provide secure/timely management of enabling/disabling user access to cloud.
- *Recommendations*. Do not use proprietary solutions; use standard connectors on service provisioning mark-up language (SPML) schema; extend authoritative data repositories to the cloud.
- *Authentication.* Utilize strong (two-factor), credentialed cloud security authentication mechanisms.
- *Recommendations*. *For SaaS/PaaS*: customer should "authenticate users via their Identity Provider and establish trust with the SaaS vender by federation" (p. 64); consider utilizing "user centric authentication" (i.e., similar to/or those used by Google, Yahoo, OpenID, Live ID) for a "single set of credentials valid at multiple sites" (p. 64); evaluate the security of this third party before use. *For IaaS*: require IT personnel use a dedicated virtual private network, similar to/or OpenID or a secure socket layer (anything OATH[194] compliant) which leverages an identity management system; ensure the cloud supports SAML[195] so that authentication is

[191] William F. Pelgrin, "*Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter*," April 2010, at: http://www.msisac.org/awareness/news/2010-04.cfm (accessed July 26, 2010).

[192] James P. Durbano, Derek Rustvold, George Saylor and John Studarus, "Securing the Cloud," *Computer Communications and Networks: Cloud Computing Principles, Systems and Applications*, (London: Springer, 2010).

[193] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 63–67.

[194] OATH stands for open authentication which is a viable single sign-on industry standard.

[195] SAML stands for Security Assertion Markup Language which is a standard for exchanging authentication/authorization data between a customer and his/her service provider.

delegated to the customer; ensure the cloud provider or private cloud uses strong authentication: "one-time passwords, biometrics, digital certificates, and Kerberos" (p. 65).

- *Federation.* Ensure secure identity management between service provider/customer and other entities (confidentiality, integrity & non-repudiation).
- *Recommendations.* Use SAML and WS-Federation[196] (prominent standards); implementing a federation gateway allows support of a variety of "federation token formats" (p. 65); a federated public single sign on (SSO) must be contrasted with a federated private SSO depending on the level of security needed and whether interaction with outside agencies is important. The DoD may consider a public SSO when interacting with other federal agencies.
- *Authorization & user profile management/access control.* Use strong access controls and associated policies to verify trusted user; consider a serial peripheral interface environment, with audit ability.
- *Recommendations.* Ensure model of access control parallels service/data; ensure authoritative policy sources align with privacy and "user profile information" (p. 66); verify enforceable policy decision via the appropriate authorities; ensure information is logged for auditing purposes; properly design identity management for compliance with regulations regarding access, e.g., segregation enforcement.[197]

General access control countermeasures.[198] Cloud computing presents innovative management consoles for access controls, as administrative privileges are delegated to common users (customers); these require specialized controls to assist in prevention of inappropriate use.[199] In addition, preventative security measures should be applied to mobile devices, including time periods for non-user accounts. Role-based

[196] WS-Federation is an identity federation specification which allows different security mechanism to collaborate on authentication and identity of disparate users.

[197] All of the information in this figure is expounded upon in the following source: Subra Kumaraswamy, Sitaraman Lakshminarayanan, Michael Reiter, Joseph Stein, Yvonne Wilson, "*Domain 12: Guidance for Identity & Access Management V2.1*," April 2010, at: http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf (accessed August 6, 2010).

[198] Vivek Kundra, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96," *CIO Council*, November 2, 2010, at https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf (accessed November 24, 2010).

[199] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

access control policies and the principle of least privilege should be integrated into assignment and authentication of user accounts. Remote access security controls should be applied to

> …establishing system accounts, configuring access authorizations, performing system administration functions, auditing system events, accessing event logs, SSH, and VPN (p. 5).

For user-based collaborative information sharing, user discretion must be clarified. Techniques such as integration of the DoD common access card or a Public Key Infrastructure certificate with cloud computing, as done by forge.mil,[200] presents additional security authentication and authorization as recommended by this domain.

Conclusions. The access control domain addressed countermeasures for frictionless registration, account hijacking, and authentication attacks such as strong or multi-factor authentication. Recommendations were provided for overarching identity and access management issues, specifically involving identity provisioning, authentication, federation, authorization and user profile management. Lastly, generic countermeasures were discussed, such as integration of access control with the DoD common access card, SAML, WS-federation, and proactive auditing and monitoring.

2. Telecommunications and Network Security

This domain discusses threats such as exploitation via cloud hacking, denial of service, and manipulation of vulnerabilities within a virtual machine, followed by countermeasures to mitigate these threats. Next, attacks and countermeasures on virtual machines vulnerabilities are discussed, followed by generic countermeasures to telecommunications and network security in the cloud.

Nefarious use of clouds. The CSA identified one of the top six threats to cloud security as hackers using a cloud's IaaS or PaaS for abuse and nefarious activity.[201] CSA predicts hackers will use cloud computing for nefarious activities such as to host

[200] This was found on Forge.com FAQs website: http://www.forge.mil/Faqs.html#faqs7.

[201] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

malware, build rainbow tables or maintain CAPTCHA[202] hacking farms, and operate botnet command and control servers.[203]

In a survey of 100 attendees at the 2010 meeting of DEFCON, an annual hacker convention held in Las Vegas, the attendees provided the following insight: 96 percent said "they believed the cloud would open up more hacking opportunities;" 45 percent admitted to hacking the cloud (12 percent hacked for financial gain); 21 percent thought SaaS was the most vulnerable aspect of cloud computing; 33 percent discovered vulnerabilities in public domain name servers, 16 percent in log files, and 12 percent in communication profiles.[204]

Countermeasures. Countermeasures to nefarious use of the cloud include:

- Increase monitoring/filtering of network traffic (using firewalls, blacklists for network blocks, intrusion detection/prevention systems, and anti-virus technology) for any unauthorized activity (e.g., credit card scams).[205]
- Scrutinize screening of cloud provider personnel;[206] require non-disclosure agreements, while limiting employee access to least privilege.[207]
- Increase stringency on registration practices.[208]
- Ensure meticulous scrutiny of a cloud provider's patch management policy and procedures.[209]

---

[202] This acronym stands for "Completely Automated Public Turing test to tell Computers and Humans Apart"

[203] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0," 8.

[204] Windsor Genova, "Cloud Software Vulnerable to Hackers, Defcon Survey Says," *International Business Times*, August 25, 2010, at: http://www.net-security.org/secworld.php?id=9773 (accessed September 10, 2010).

[205] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0," 8.

[206] Ibid.

[207] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 50.

[208] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0," 8.

[209] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 52–53.

- Verify the cloud provider "restrict[s] data ingress/egress points…to mitigate the introduction of malicious software and removal of private data."[210]
- Confirm that a cloud provider scans, isolates and replaces any questionable instances on the cloud.[211]
- Conduct audits of resource usage to assist in detection of malicious use on the cloud.[212]

Denial of service (DoS) attack.[213] Some security experts purport that cloud computing is more susceptible to a DoS attack, negatively impacting service availability, due to the multi-hosted nature of the network.[214] The implication is that once one partition is affected, other partitions will also be negatively affected due to the multi-tenant nature of cloud computing. Two real-world incidents include: (1) One Georgian blogger with multiple accounts on Twitter, Facebook, Live Journal, Google's Blogger and YouTube was the target of a DoS that took down Twitter's entire site for several hours and slowed service.[215] (2) During October 2009, Amazon cloud customer Bitbucket experienced a 19-hour outage during a distributed DoS attack.[216] According to one of Bitbucket's operators, the company was attacked with a "flood of UDP [user datagram protocol] packets coming into our IP [internet protocol], basically eating away all bandwidth;" the attack created latency in reading documents stored on Bitbucket's EBS [elastic block storage].[217]

---

[210] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud," 8.

[211] Ibid.

[212] Ibid.

[213] A DoS attack consists of an attempt to send excessive traffic to a network in order to overwhelm/disable and in turn deny access to that network website/server or service.

[214] Gregg, "Ten Security Concerns for Cloud Computing."

[215] Elinor Mills, "Twitter, Facebook Attack Targeted One User," *Cnet News*, August 6, 2009, at: http://news.cnet.com/8301-27080_3-10305200-245.html (accessed September 10, 2010).

[216] Liam Eagle, "DDoS Attack Hits Amazon Cloud Customer Hard," *Web Host Industry Review*, October 6, 2009, at: http://www.thewhir.com/web-hosting-news/100609_Outage_Hits_Amazon_Cloud_Customer_Hard (accessed August 16, 2010).

[217] Eagle, "DDoS Attack Hits Amazon Cloud Customer Hard," 1.

Countermeasures. Some of the countermeasures against a DoS attack within a cloud include: "authentication, authorization, filtering, throttling, and quality of service."[218] (ISC)2 provides generic recommendations for DoS attacks:

> multiple layers of firewalls, careful filtering on firewalls, routers and switches, internal network access control (NAC), redundant (diverse) network connections, load balancing, reserved bandwidth (quality of service, which would at least protect systems not directly targeted), and blocking traffic from an attacker on upstream router.[219]

Ensure the cloud provider restricts "dynamic utilization of resources" to set levels to counter internal denial-of-service attacks.[220] The SLA should stipulate that the provider identify all DoS or distributed DoS attack methods, and establish measures (which are audited and verified) to mitigate such attacks.

Attacks on virtual machine (VM) vulnerabilities (hypervisor/management components, and hardware backplane):[221] Cloud uses virtualization technology that is not protected by standard network security controls; virtual operating systems often lack "security-by-default" implementations.[222] Without standard security controls, cloud solutions experience certain unique attacks. More specifically, a guest-hopping attack occurs when a hacker attacks a "resource isolation mechanism" (i.e., a hypervisor) that is used to separate "storage, memory [or] routing."[223] This vulnerability was announced by

---

[218] Ragib Hasan, "*Security and Privacy in Cloud Computing*," John Hopkins University Lecture Slides, February 1, 2010, at: http://www.cs.jhu.edu/~ragib/sp10/cs412/lectures/600.412.lecture02.pdf (accessed September 10, 2010).

[219] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 745.

[220] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud," 7.

[221] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 68–69.

[222] Ibid.

[223] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," 9.

the U.S. CERT as vulnerability CVE-2009-3733, a.k.a the "traversal vulnerability," which states an attacker can traverse from one VM client environment to another if managed by the same hypervisor.[224]

Countermeasures/recommendations:[225] Incorporate layered security controls (i.e., intrusion detection/protection systems (IDS & IPS), firewalls, anti-virus and vulnerability scanning tools) as well as compartmentalization on VMs to protect management components, hypervisors, and hardware backplane; decrease reliance on the security of a cloud provider alone. Ensure quality and pedigree of a cloud provider's VM before use. Create security zones to separate VMs into categories based on: (1) type of use, (2) stage of production, and (3) data sensitivity. Ensure methods of reporting are in place in case of an isolation breach. Ensure regulations on VM isolation requirements are adhered.

In order to provide boundary protection, any transmitted information must undergo inspection by Trusted Internet Connection processes.[226] All internal communications should be routed via "authenticated proxy servers."[227] The provider must define

> …key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.[228]

Transmission confidentiality should be protected with a "hardened or alarmed carrier protective distribution system" when cryptography cannot be used.[229] The provider must

---

224 U.S. Computer Emergency Response Team, "*Vulnerability Summary for CVE-2009-3733*," November 2, 2009, at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3733 (accessed September 10, 2010).

225 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 68-69.

226 Kundra, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96."

227 Ibid., 28.

228 Ibid.

229 Kundra, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96," 29.

define where trusted paths exist, e.g., "system authentication, re-authentication, and provisioning of services," i.e., bandwidth, in order to align appropriate controls where necessary.[230]

Conclusions. This domain addressed the relevant issues and countermeasures to cloud hacking, DoS and VM attacks. Next, other generic countermeasures in this domain were outlined. Boundary protection is paramount both within and outside of the cloud, and the provider must ensure that provisions protect the CIA of a customer's data. Some of these measures include internal/external layered security controls such as IDS & IPS, as well as compartmentalization of virtual instances in order to protect dispersive system components.

3. Information security governance and risk management

The focus of analysis within this domain will center on information security policy as well as risk management/assessment, both of which are administrative security controls. From there, countermeasures are outlined in strengthening the CIA of data.

Fragmented and incomplete security guidance of cloud computing implementation might result in exploited vulnerabilities. Governance is defined as a "structure of relationships and processes" which provides an enterprise direction toward its goals.[231] Comprehensive security guidance or governance for implementation of cloud computing is "fragmented between agencies and so far incomplete."[232] Individual efforts by ENISA, CSA, NIST, the Office of Management and Budget, and GSA are in progress, but "far from complete."[233]

---

[230] Kundra, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96," 29.

[231] Tipton, *Official (ISC)2Guide to the CISSP CBK*, 411.

[232] Jackson, "Security Must Come Before the Cloud, GAO Says."

[233] Eric Chabrow, "*Can Cloud Be More Secure Than Legacy Systems?*" Government Information Security Articles, July 1, 2010, at: http://www.govinfosecurity.com/articles.php?art_id=2714&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GovinfosecuritycomRssMain+%28GovInfoSecurity.com+RSS+Main%29 (accessed September 10, 2010).

Loss of security compliance and regulation to a third party provider. By allowing a third party to manage a cloud, a customer loses direct control of security, and thus compromises the CIA of its data and operations.[234] Even in managing its own private cloud, the DoD will need guidance and rules on securing a cloud computing infrastructure, and this is currently in development.

Countermeasures for fragmented governance and compliance issues include:

(1) "Federal guidance and processes" must specifically address security controls to ensure a secure solution for sharing resources.[235] Agencies must continue to unite and produce consolidated guidance for securing the cloud. These efforts are in progress and are beginning to bear fruit.

(2) The DoD should stipulate governance requirements in an SLA and audit regularly to ensure the cloud provider is adhering. The application of security policy to a cloud computing solution should not be an afterthought, but rather part of the process during initial planning.[236]

(3) CSA created a Cloud Control Matrix which outlines security policies for cloud solutions.[237] This matrix aligns security controls for cloud computing with corresponding policies, e.g., Compliance (Audit Planning) aligns with HIPAA 164.312(b), ISO/IEC 27002-2005 15.3.1, NIST SP800-53 R2 CA-7, and NIST SP800-53 R2 PL-6.

(4) Overarching security policies should be considered (see Figure 1).

---

[234] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," 9.

[235] Jackson, "Security Must Come Before the Cloud, GAO Says."

[236] David Linthicum, "*Three Cloud Computing Mistakes You Can Avoid Today*," MISAsia, March 12, 2010, at: http://mis-asia.com/cio_focus/technology/3-cloud-computing-mistakes-you-can-avoid-today (accessed September 10, 2010).

[237] On the CSA website, http://www.cloudsecurityalliance.org/, click on "Download Control Matrix" on right hand side of webpage under "NEW RESEARCH." Current as of August 6, 2010.

Control Objectives for Information and related Technology (COBIT®), Version 4.1 (2007)	http://www.isaca.org
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules	http://www.hhs.gov/ocr/privacy/
International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27002:2005 -- IT -- Security techniques -- Code of practice for Information Security Management	http://www.iso.org/iso/iso_catalogue.htm
National Institute of Technology (NIST) Special Publication 800-53 -- Recommended Security Controls for Federal Information Systems, Revision 2 (Dec 2007)	http://csrc.nist.gov/publications/PubsSPs.html
Payment Card Industry (PCI) Data Security Standard (DSS) Requirements and Security Assessment Procedures, Version 1.2 (Oct 2008)	https://www.pcisecuritystandards.org/index.shtml
Other Compliance Resources	
NIST Special Publications (800 Series)	http://csrc.nist.gov/publications/PubsSPs.html
International Standards • ISO/IEC 27003:2010, IT -- Security techniques -- Information security management system implementation guidance • ISO/IEC 27033-1:2009, IT -- Security techniques -- Network security -- Part 1: Overview and concepts • ISO/IEC 19792:2009, IT -- Security techniques -- Security evaluation of biometrics • ISO 31000:2009, Risk management -- Principles and guidelines • ISO 9001:2008, Quality management systems -- Requirements • ISO 14001:2004, Environmental management systems - Requirements with guidance for use • ISO 27799:2008, Health informatics -- Information security management in health using ISO/IEC 27002 • BS 25999:2007, Business continuity management	http://www.iso.org/iso/iso_catalogue.htm
Generally Accepted Privacy Principles (GAPP)	http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/
Health IT for Economic and Clinical Health (HITECH) Act passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA)	http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html
BITS Shared Assessments Program Agreed Upon Procedures (AUP) Version 5.0 Assessment Guide	http://www.sharedassessments.org/

Figure 1. Overarching Cloud Computing Governance Resources[238]

[238] On the CSA website, http://www.cloudsecurityalliance.org/, this chart was cut and pasted from data found in the CSA Cloud Control Matrix, compliance reference matrix tab.

(5) On July 30, 2010, the Assistant Secretary of Defense built a DoD IA Policy Chart that aggregated all policies necessary for orchestrating a trusted global information grid.[239] While generic to IA, this chart (see link in footnote) can be applied to cloud security.[240] The chart lists regulation guidance for securing data in transit (section 2.1), managing access (section 2.2), assuring information sharing (section 2.3), preventing and delaying attackers (section 3.2), preventing attackers from staying (section 3.3), and developing and maintaining trust (section 4.1) to list a few.[241]

(6) NIST promotes "the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards."[242] NIST recently created the cloud computing security group for guidance and standards in securing the cloud.[243] Since cloud computing is growing in popularity, NIST is beginning to release relevant publications. In a report in October 2009, NIST articulated their roadmap and way ahead as defining minimal standards with each cloud model.[244]

(7) On November 2, 2010, the White House provided a draft of requirements for securing cloud computing within the federal government, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing," which used NIST Special Publication 800-53R3 as a foundation for the security controls outlined.[245] These security controls can be used to guide the DoD once finalized.

---

[239] Chart by Deputy Assistant Secretary of Defense, "*Cyber, Identity & Information Assurance (CIIA) Related Policies and Issuances: Build and Operate a Trusted GIG*," July 30, 2010, at: http://iac.dtic.mil/iatac/download/ia_policychart.pdf (accessed September 10, 2010).

[240] Ibid., 1.

[241] Chart by Deputy Assistant Secretary of Defense, "Cyber, Identity & Information Assurance (CIIA) Related Policies and Issuances: Build and Operate a Trusted GIG," 1.

[242] Harauz, "Data Security in the World of Cloud Computing," 64.

[243] National Institute for Standards and Technology Website, Computer Security Division: Computer Security Resource Center, May 11, 2009, at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010).

[244] Mell and Grance, "Effectively and Securely Using the Cloud Computing Paradigm," slide 45.

[245] Chabrow, "White House Issues Secure Cloud Computing Guidance: FedRAMP Requirements aimed to easy cloud computing adoption."

(7) Some general recommendations/countermeasures on governance in cloud computing include:[246]

- Periodically inspect to verify a cloud provider's security capability and controls to ensure security requirements are met, and documented into an SLA.
- The customer and cloud provider must agree on goals to support mission objectives on information security governance, roles, responsibilities, and accountability.
- Inspect a cloud provider's security governance to ensure it is sufficient, mature and consistent with DoD security management processes.
- Ensure an external provider uses standards and metrics to monitor security management performance.

Failures in risk management. Information risk management involves identifying and assessing risks, reducing those risks to an acceptable level, and then implementing countermeasures to maintain that level.[247] Risks that involve physical damage, human interaction, equipment malfunction, inside and outside attacks, data misuse or loss, and errors within applications could easily negatively impact DoD operations reliant on cloud computing.[248] In research conducted by the Information Systems Audit and Control Association (ISACA), which spans Europe, Africa and the Middle East, 25 percent of organizations using cloud computing believe the risks outweigh the benefits for cloud computing, yet continue use.[249]

Countermeasures.

(1) Research benefits and risks in a formal risk management process prior to implementation, and specify this process in an SLA if using an external provider.[250] This risk assessment will likely reveal a need for encryption/classification of data, proper

[246] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 31–34.

[247] Ibid.,73.

[248] Ibid.

[249] HelpNet Security, "Cloud Computing: Risks Outweigh the Benefits," March 23, 2010, at: http://www.net-security.org/secworld.php?id=9051 (accessed September 10, 2010).

[250] Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

authentication, monitoring for intrusions, and redundancies/back-ups for continuity of service.[251]

(2) Ensure the cloud provider notifies the customer of how risks are mitigated or handled.[252] For a DoD private cloud, this may entail notifying the chain of command.

(3) Ensure cognizance of an ENISA risk assessment report on cloud computing that outlines risks, vulnerabilities and challenges with associated solutions and recommendations.[253] The latest ENISA report, 2009, creates a checklist of security-related questions aimed at meeting business needs of customers.[254] These risks are highlighted below.[255]

- *Loss of Governance*: customer cedes security governance to a cloud provider
- *Lock In*: a customer of cloud is locked into using a provider due to lack of interoperability between providers
- *Isolation Failure*: storage, memory and routing are traversed by unauthorized users
- *Compliance*: a cloud provider may not provide evidence of security certifications required by DoD instructions
- *Management Interface Compromise*: unauthorized access is gained via web browser/remote access vulnerabilities
- *Data Protection*: data is mishandled and an unauthorized person gains access to proprietary information
- *Insecure Data Deletion*: wiping of data is not done correctly or completely
- *Malicious insider:* a system administrator uses access for malicious purposes

---

[251] Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

[252] DePompa, "The Cloud's Standard Imperative."

[253] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," 9–10.

[254] Giles Hogben, "ENISA Clears the Fog on Cloud Computing Security," *European Network and Information Security Agency*, November 20, 2009, at: http://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1/?searchterm=cloud%20security (accessed September 10, 2010).

[255] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," 9–10.

(4) Incorporate CSA guidance on risk management:[256]

- Lack of physical control over infrastructure mandates a more significant role for SLAs and contractual agreements. Analyze and identify assets, threats and vulnerabilities in order to establish risk management plans and assessments, with outcomes identified in SLAs.
- Due to on-demand provisions with multi-tenant architectures, integrate alternatives for vulnerability assessments and penetration tests.
- Ensure meticulous management and accountability of all equipment supporting cloud implementations.
- Investigate a cloud provider's supplier security process chain for incident management, business continuity, security metrics, and policy compliance.
- Request documentation and validation of security assessments on facility and services to thoroughly investigate risk, frequency of occurrence, and timely mitigation.
- Ensure cloud provider practices due diligence in terms of: financial status, reputation, security controls, personnel hiring, business continuity, insurance, and service capability.

(5) Comply with federal government processes for risk management. The Federal Risk and Authorization Management Program, a.k.a. FedRAMP, is an attempt to enable adoption of cloud computing through a government-wide authorization process.[257] In 2009, a Cloud Computing Advisory Council (CCAC) was formed to start FedRAMP by the Federal Chief Information Officer. FedRAMP is voluntary because many agencies already conduct validated processes to accredit their systems; the intent of the program is to provide oversight without duplication of effort.[258] The CCAC president is calling FedRAMP a "unified, risk management program" which enables common security requirements for federal agencies, compatible security requirements, cost savings/lack of duplication of effort, expedient acquisition of cloud services due to pre-authorized

[256] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 31–34.

[257] Eric Chabrow, "Balancing Act: Security Meets Functionality," *Government Information Security Articles*, December 14, 2009, at: http://www.govinfosecurity.com/articles.php?art_id=2005 (accessed May 17, 2010).

[258] Chabrow, "Balancing Act: Security Meets Functionality."

packages—providers will now work with one authorization body for risk management;[259] and thus, increase interoperability of government security efforts.[260]

Conclusions. The information security governance and risk management domain brought to light that security guidance for cloud computing is currently incomplete and fragmented. Additionally, security compliance with cloud computing often involves outsourcing security compliance/regulation to a third party provider. For these reasons, federal and DoD guidance will need to address security controls, and these controls will need to be outlined in SLAs with third parties. This chapter also presented overarching Information Assurance security policies and governance resources upon which to build. It highlighted a new draft document from the White House, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing," and processes which, once finalized, can be capitalized upon by the DoD. Following, failures in risk management were addressed with recommendations and countermeasures. Overall, this chapter showed the need for more governance in securing cloud solutions, as well as the need to conduct meticulous risk management for implementations of this new technology.

4. Application Security

When dealing with application security, the DoD must consider the three levels of cloud computing, PaaS, SaaS and IaaS. This chapter will delve into security issues with insecure interfaces, and then specific security issues within each of the three cloud levels, followed by countermeasures and recommendations.

Exploitation of insecure interfaces[261] and application programming interfaces (APIs). CSA lists insecure or weak interfaces and APIs as a top threat to cloud security.[262] Interfaces for access control, encryption, and activity monitoring must

[259] Chabrow, "Balancing Act: Security Meets Functionality."

[260] Ibid.

[261] An interface is a point at which components interact whether on software or hardware level.

[262] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

encompass secure designs to prevent malicious and accidental circumventions of security policy.[263] Risks to APIs increase when providers continually add services for customers. Examples of weak APIs include:

> Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.[264]

Countermeasures. The DoD should analyze and validate: (1) the security model for interfaces, (2) the strength of access control and authentication integrated with encryption, (3) all API dependency chains,[265] and (4) whether server partitions between VMs are impermeable, isolating data on its own physical server (isolation management) if not.

Exploitation of insecure application architectures within PaaS, SaaS, and IaaS. Several of the areas of concern with securing application architectures involve: message communication, information handling, key management, software development lifecycle (SDLC), tools and services, metrics, inter-host communication and economics.

Countermeasures. In non-cloud environments, "debug and audit logging" usually span to local storage, but with a cloud solution, these services must now permeate to remote arenas.[266] Specific countermeasures for PaaS, SaaS, and IaaS include:

PaaS: PaaS providers should integrate "built-in application security controls" in the programming sections to assist developers in avoiding common application vulnerabilities.[267] Additional PaaS vulnerabilities and associated countermeasures include:[268]

---

[263] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

[264] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

[265] Ibid. Ibid cannot be first footnote on a page

[266] John Arnold, "Domain 10: Guidance for Application Security V2.1," *Cloud Security Alliance*, July 2010, at: http://www.cloudsecurityalliance.org/guidance/csaguide-dom10-v2.10.pdf (accessed August 21, 2010), 7.

[267] Ibid., 15.

[268] Ibid., 15–17.

- *Secure Message Communication*. Multi-tenancy mandates reevaluation of trusted paths within two layers: (1) integration and middleware, and (2) API. For messages, WS-Security[269] should be used.
- *Sensitive Information Handling*. When "data is logged for debugging purposes," use "application provided cryptographic controls" (p. 16). Ensure compliance with regulations on audit log retention.
- *Application Key Management*. Securely manage application keys and credentials.
- *SDLC*. Secure PaaS platform and ensure provider follows a secure SDLC.
- *Tools and Services*. Use Open Web Application Security Project (OWASP) to gain awareness on web-based/n-Tier application vulnerabilities/countermeasures.

SaaS: SaaS areas of concern and countermeasures include:[270]

- *SDLC*. Challenges arise with delineation between cloud provider and application owner responsibilities on implementing security software development measures. Use the SLA to negotiate changes in trusted boundaries and request documentation of security measures, testing, logging, audit reporting and periodic inspection of security controls.
- *Metrics.* Require security metrics from third party cloud provider.
- *Tools and Services*. Utilize customizable Web Application Firewalls (WAF) or a distributed WAF across hardware, CPU[271] and server/datacenter boundaries with minimal network disruption.
- *Economics.* Providers should provide strong application security to reduce breaches, and increase quality of service.

IaaS: IaaS vulnerabilities and countermeasures include:[272]

- *Secure Application Architecture*. Utilize infrastructure controls (as they do not exist by default) at the configuration and application level.
- *Trusted Virtual Machine Image.* Hardening of all images and verification of security must equal or surpass that of traditional hosts. A security

[269] WS-Security or web services security is a protocol used to ensure confidentiality and integrity of messages.

[270] Arnold, "Domain 10: Guidance for Application Security V2.1," 17–20.

[271] CPU or central processing unit is the portion of the computer system which implements instructions of a computer program.

[272] Arnold, "Domain 10: Guidance for Application Security V2.1," 20–22.

incident can take place if a compromised OS[273] is uploaded to the cloud without proper security verification.

- *Hardening Hosts*. Incorporate equal security measures for hardening hosts in the DMZ to virtual images. Incorporate DMZ and cloud-based applications with "custom operating system implementations and application platform images which only have the capabilities necessary to support the application stack" (p. 21). Decreasing application stack capabilities and attack surfaces reduces the number of patches necessary to secure the host.
- *Securing Inter-host communication*. Do not permit platform administrators of the physical infrastructure unequivocal access to internal administration of data.
- *Application Key Management*. Modify best practices for secure key handling to management of IaaS platform keys.
- *Handling Sensitive Data*. In order to prevent data leakage, apply filtering and masking to "operations, exception handling and audit logging" (p. 22).
- *SDLC*. Security guidance from CSA needs updating in (1) application trust/threat models, (2) assessment tools for application security, and (3) guidance on changes to application security architecture.

Conclusions. The application security domain addressed exploitation and countermeasures to protect insecure interfaces. It provided methods of increasing security for PaaS, SaaS, and IaaS, in the realm of message communication, information handling, key management, SDLC, proper tools and services, metrics, economics, and inter-host communication.

5. Cryptography

Cryptography and key management within the cloud is utilized to protect the confidentiality and privacy of data, as well as its integrity. This chapter covers exposure of confidential data via cryptographic attacks and countermeasures, discussion of FBI plans to require providers to expose encryption keys, exploitations of data encryption, recommendations for in transit and at rest data encryption, key management issues, generic encryption recommendations, and homomorphic encryption.

[273] OS or operating system.

Disclosure of confidential data via various attacks. Data requires encryption before placement on the cloud if confidentiality is a concern.[274] Steganographic techniques can also used to hide or transform data to prevent exposure.[275] In a recent publication "Trusting the Cloud," three researchers proposed data protection through "well-known cryptographic methods."[276] However, even if data is encrypted, it may be vulnerable to attack if the encryption is weak, poorly implemented, or fails to take into account sophisticated attacks such as man-in-the middle and side channel attacks. In a man-in-the-middle attack, an attacker places herself between two users to intercept or modify the messages transmitted, decrypting and re-encrypting data in the process.[277] In a side-channel attack, an enemy/attacker places a malicious virtual machine close to a targeted machine in order to acquire data that can be useful for cracking encryption keys.[278]

In addition to confidentiality protection, data integrity can be verified by storing a hash "in local memory and authenticating server responses by re-calculating the hash of the received data and comparing it to the locally stored value."[279] Availability and integrity of data can be verified by using Proofs of Retrievability and Proofs of Data Possession; these protocols assure a client can retrieve personal data "with high probability."[280]

---

274 Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

275 Kumar and Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy," 1–14.

276 Christian Cachin, Idit Keidar, and Alexander Shraer, "*Trusting the Cloud*." ACM SIGACT News, 2009: 83.

277 Gregg, "Ten Security Concerns for Cloud Computing."

278 Ibid.

279 Cachin, Keidar and Shraer, "Trusting the Cloud," *ACM SIGACT News*, 2009: 83.

280 Ibid.

FBI surveillance requirements. There are concerns that a new legislative proposal for an upgraded FBI surveillance program might create security issues for cloud computing.[281] The proposal requires that (1) communication firms unscramble encrypted messages; (2) foreign companies perform intercepts on information in U.S.-based offices; and (3) companies with peer-to-peer services redesign their infrastructure to allow message intercept.[282] This new proposal might enable the government to have access to encryption keys, placing data at risk for compromise. Overall, message security and encryption keys/processes could be more exposed/vulnerable. This policy may require threat assessment/mitigation to secure data in the cloud.

Other exploitations of data encryption. In cloud computing, a nefarious user can potentially view file systems and volatile memory images stored to disk when "copying off a dormant image of an instance."[283] It is possible that confidential information which is "normally encrypted on disk but not in memory, may end up stored on disk in an unencrypted format."[284] Additional controls are necessary to encrypt instances when stored to disk and during migration between servers.[285]

In transit, at rest and backup encryption recommendations. Data should be encrypted while in transit across networks in the cloud, which can be done with ease across SaaS, PaaS, and IaaS platforms.[286] Additionally, encryption of data at rest protects against malicious provider personnel or co-tenants, as well as application abuse.[287] At rest encryption is commonly available for an IaaS via provider tools, but more difficult with PaaS, since customization is required; cloud customers cannot directly

---

[281] Alex Williams, "Why the FBI's Surveillance Proposal Could Be a Disaster for the Cloud," *ReadWriteCloud*, September 28, 2010, at: http://www.readwriteweb.com/cloud/2010/09/why-fbi-surveillance-disaster.php (accessed October 1, 2010).

[282] Williams, "Why the FBI's Surveillance Proposal Could Be a Disaster for the Cloud."

[283] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud," 5.

[284] Ibid.

[285] Ibid.

[286] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1."

[287] Ibid.

implement encryption for data at rest in SaaS, but must request help from a provider.[288] Many cloud providers encrypt data for backup media transparently; this prevents unauthorized access to lost or stolen media.[289]

Key management issues. Customers need to ensure that countermeasures are taken with key security, access, and recoverability/backup. These include (1) adherence to standards for key management: OASIS Key Management Interoperability Protocol, and IEEE 1619.3;[290] (2) protection of keys in storage, transit and backup;[291] (3) restricted access to keys based on need-to-know and separation of roles;[292] and (4) use of backup and recovery processes for keys in case of accidental loss or intentional destruction.[293]

Other encryption recommendations. Some of the following encryption recommendations can create more security for a cloud solution: Use encryption to separate data usage and holding.[294] Ensure that key management is separated from the cloud provider.[295] Ensure encryption processes adhere with industry, DoD and government standards.[296] Ensure role management and separation of duties is implemented with encryption processes.[297] Ensure customers are issued different keys, and that the cloud provider (if key management is delegated) has a documented process for lifecycle management of encryption keys.[298] In order to provide non-repudiation, use FIPS 140-2 "cryptography (e.g., DoD PKI Class 3 or 4 tokens) for service offerings

---

[288] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1."

[289] Ibid.

[290] Ibid.

[291] Ibid.

[292] Ibid.

[293] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1."

[294] Ibid.

[295] Ibid.

[296] Ibid.

[297] Ibid.

[298] Ibid.

that include SaaS with email."[299] The provider should define the PKI certificate policy, and ensure it is validated by an official approval authority, such as the designated approval authority.[300]

Homomorphic encryption. An IBM researcher recently created a homomorphic encryption scheme which allows data to be processed in an encrypted state.[301] IBM asserts that this solution could be used in the future to strengthen the security of cloud computing; it would enable providers to "perform computations on data at their clients' request without exposing the original data."[302] Although current methods are not practical, it is an area of research with potential benefits.

Conclusions. Traditional encryption processes can transfer to the cloud, including encryption for confidentiality protection, hashing for data integrity, and proofs of retrievability/data possession for integrity and availability. Government surveillance legislation can propose risk to data confidentiality for national security purposes, and this will affect the cloud along with other information systems. Cloud customers will need to ensure processes are implemented to encrypt their data in transit, at rest, and for backup purposes. Additionally, key management should adhere to security standards, need-to-know, and separation of duty controls. Other generic recommendations for cloud encryption were presented, along with the potential security enhancements that could come with homomorphic encryption if practical methods are found. Overall, the cryptographic domain provided valuable insights into how the confidentiality of customer data is protected.

---

[299] Vivek Kundra, "Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96," 9.

[300] Ibid., 30.

[301] Brian Prince, "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering," *E-Week.com*, June 25, 2009, at: http://www.eweek.com/c/a/Security/IBM-Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/ (accessed November 24, 2010).

[302] Prince, "IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering," 1.

6. Security Architecture and Design

In order to closely monitor resources for unauthorized activities or accesses,[303] cloud customers should verify that proper security coding practices are utilized in cloud architecture designs.[304] This chapter summarizes potential problem areas within cloud to include: shared technologies, failures in design, and authorization.

Exploitation of shared technology issues. CSA identified "shared technology issues" as a major threat to cloud security; the vulnerability is that "disk partitions, CPU caches, GPUs, and other shared elements were not designed for strong compartmentalization."[305] Without strong barriers to isolate and protect the "multi-tenant architecture" inherent in cloud computing, guest operating systems can obtain inadvertent control and influence over other platforms.[306]

The National Vulnerability Database lists exploitation of shared technology issues as a "directory traversal vulnerability…,[which] allows remote attackers to read arbitrary files via unsuspected vectors."[307] Examples of these types of attacks are "Joanna Rutkowska's Red and Blue Pill exploits, and Kortchinsky's CloudBurst presentations."[308]

Remediation or countermeasures to this threat include: performing configuration audits and vulnerability scans; enforcing patching and rectification of vulnerabilities in SLAs; utilizing strong authentication and access control for any operation; monitoring for unauthorized changes and malicious activity; isolation management, and implementing best practices for configuration and installation.[309]

---

303 Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

304 Barbara DePompa, "The Cloud's Standard Imperative."

305 Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

306 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1."

307 U.S. CERT, National Vulnerability Database, Vulnerability Summary for CVE-2009-2902, at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2902 (accessed November 24, 2010).

308 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1."

309 Ibid.

Failure to design for demand results in loss of availability. Problems arise for the cloud provider when security architecture is not properly planned. A vendor is required to accurately estimate demand for service; when there is error in this calculation and a cloud reaches 80 percent capacity or more, servers thrash during movement of "data between disks and local memory" resulting in unresponsive computers.[310] The resulting outage incurs financial and reputation deficits to both cloud provider and customer.[311]

Providers should design their security architecture in consideration of (1) accurate estimates of customer demand, (2) sufficient slack resources for situations of overcapacity and/or restriction of requests for more capacity when established limits are reached.[312] When a customer assesses bids for cloud computing, the customer should assess the cloud provider's design capacity to enable continuous operations.

Authorization. Certification and accreditation is a significant topic in the security architecture and design domain. Currently, the DoD uses the DoD Information Assurance Certification and Accreditation Process (DIACAP) to ensure information systems meet secure design criteria, as approved by a designated approval authority. Cloud computing will also need to follow this paradigm. The federal government just submitted a first draft of their proposed assessment and authorization process.[313] The first chapter outlined security baseline requirements for cloud, founded upon NIST Special Publication 800-53R3.[314] The second chapter described how clouds will be monitored and held accountable for compliance with FISMA, Federal Information System Management Act of 2002.[315] Chapter three described a potential assessment and authorization approach involving a joint authorization process with DoD sitting in as an

---

[310] Paquette, Jaeger, and Wilson, "Identifying the security risks associated with governmental use of cloud computing," 251.

[311] Ibid.

[312] Paquette, Jaeger, and Wilson, "Identifying the security risks associated with governmental use of cloud computing," 251.

[313] Eric Chabrow, "White House Issues Secure Cloud Computing Guidance: FedRAMP Requirements aimed to easy cloud computing adoption."

[314] Ibid.

[315] Ibid.

approval chair, all of which are based on NIST Special Publication 800-37R1.[316] While in draft form, the DoD could potentially leverage this federal process, once in place, for meeting certification and accreditation requirements, as to not re-invent the wheel.

Conclusions. The security architecture and design of a cloud computing solution dissected several important areas: establishing isolation management within shared technologies; designing architectures for meeting customer demands for service and availability; and certifying and accrediting systems before use, while leveraging federal solutions.

7. Operational Security

The domain of operations security (OPSEC) is concerned with the protection and control of distributed and centralized assets, and the daily tasks necessary to keep services operating securely, reliably and efficiently.[317] The following section describes areas of OPSEC that could be problematic in a cloud environment: patching; logging, monitoring and audit; and malicious insiders. For these areas, methods of risk mitigation are suggested.[318] Following, generic OPSEC practices are provided.

Patching. Patching is more complicated with cloud computing, as the underlying cloud infrastructure must be patched as well as the individual user instances.[319] The DoD should ensure that a cloud provider patches the "underlying host operating system (hypervisor) without impacting the virtualized servers running on that host."[320] If an instance is offline during normal patching, processes should be in place to patch these instances automatically when they come back online.[321]

---

316 Chabrow, "White House Issues Secure Cloud Computing Guidance: FedRAMP Requirements aimed to easy cloud computing adoption."

317 Tipton, *Official (ISC)2 Guide to the CISSP CBK.*

318 Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

319 Ibid.

320 Ibid.

321 Ibid.

Logging, monitoring and audit. Cloud environments introduce new arenas for logging and monitoring. The DoD should ensure the hypervisor is monitored, as well as activity associated with physical servers and virtual instances.[322] The distributed nature of cloud computing makes log processing difficult, yet important.[323]

It is especially critical to monitor virtual instances of operating systems, as they are often created with little oversight or audit accountability.[324] In addition, virtual infrastructures within a cloud computing datacenter can be initiated without physical access to the network, allowing the creation of rogue VMs that can be used for side channel attacks.[325] Virtualization can also negate application and location-based naming conventions, which in turn creates logging and tracking problems.[326] To mitigate these problems, cloud providers should introduce controls to track newly created virtual assets; and create/implement standard naming conventions for servers (vice application or location conventions) for accurate logging and tracking.[327] They should incorporate procedures to audit systems when creating virtual instances and each time a virtual instance comes online.[328]

Malicious Insiders. CSA lists a top threat to cloud security as malicious insiders.[329] Part of the concern stems from the need of cloud personnel to maintain high levels of access privilege in order to operate, maintain, monitor and audit the systems.[330] A malicious insider (working for the cloud provider) could misuse this privilege and take actions that negatively impact business operations through brand, monetary and

---

[322] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[323] Ibid.

[324] Ibid.

[325] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[326] Ibid.

[327] Ibid.

[328] Ibid.

[329] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

[330] Perry, "Security for Cloud Computing."

productivity losses.[331] For the military, this could involve compromising secret operations during war.

Some specific methods to mitigate the risk of malicious insiders include:

- Enforce stringent supply chain management, conduct thorough assessments of providers, enforce human resource criteria in SLAs, require compliance accountability through reporting, mandate transparency in security management, and require a security incident reporting process.[332]
- Ensure all supply chain management personnel meet training requirements outlined in DoD 8570.01-M, IA Workforce Improvement program.[333]
- Require industry certifications for cloud security personnel. CSA launched the Cloud Certificate of Security Knowledge program, a new standard for cloud security personnel aimed to increase professional knowledge.[334] The DoD should specify requirements to obtain this certification in their SLAs.
- Revoke server privileges immediately upon terminating an employee.
- Require security checks when hiring individuals. For example, Google Data centers holding federal information require that "security checks of datacenter employees will be done in conjunction with specific government agencies."[335]
- Do not place data on the cloud which could compromise operational security. For example, the Army Experience Center's cloud solution does not place

[331] Hubbard and Sutton, "Top Threats to Cloud Computing, V1.0."

[332] Ibid.

[333] Perry, "Security for Cloud Computing."

[334] Cloud Security Alliance Website, at: http://www.cloudsecurityalliance.org/pr20100728.html (accessed July 10, 2010).

[335] Claburn, "Google Plans Private Government Cloud."

social security numbers or personally identifiable information on forge.com.[336]

- Use role-based access controls within the cloud for privileged, ordinary, operator, system/security administrators, and Help Desk personnel in conjunction with clearances and continual account validation processes.[337]
- Restrict access to consoles (physical and virtual) to least privilege.[338]

Some general methods to mitigate risks to overall operational security include:

(1) Operational resilience.[339] In order to successfully overcome common threats to smooth operations, a cloud's vital system components must be evaluated based on mean time to failure. Trusted paths[340] should be validated using "log collection and analysis, vulnerability scanning, patch management and system integrity checking" (p. 545). Redundancies within cloud infrastructures (staffing, server, network, power supplies, drives, storage, spares, and backup/recovery systems) should be automatically integrated to ensure any system disruption goes unnoticed for cloud customer operations.

(2) Asset protection.[341] Information assets that are assigned to a cloud might not be protected at a level commensurate with their value. The DoD should stipulate the value of tangible and intangible assets to ensure controls are appropriately integrated with cloud solutions; this can be accomplished by using a classification system. All assets should be considered, including data,

---

[336] Bill Rigby, "An Interactive eBook: Cloud Computing," *Computer World*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

[337] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

[338] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[339] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

[340] A trusted path is an aspect of resiliency because it provides a "trustworthy interface into privileged user functions" to prohibit any interception or corruption. Moreover, user log in credentials are securely transmitted from "user interface to the access control subsystem." (source: Tipton, 544).

[341] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

software, classification markings, and devices. Mandatory and discretionary access controls should be integrated into the cloud as applicable.[342]

(3) *Managing security services and technologies*.[343] Diverse technologies in the cloud are required to control "change, configuration, incident and problem management."[344] Security operations involve monitoring security technologies (intrusion detection and prevention systems, firewalls, email security services) to ensure they are effective in maintenance of a reliable and resilient cloud. These technologies should integrate with cloud to establish boundary controls (separation of trusted and untrusted virtual instances); monitor and report (audit logs, security event management, log management), intrusion detection/prevention (detect and prevent attacks with signature matching, protocol/statistical anomaly, and heuristics), vulnerability management systems (find vulnerabilities in network, host and application systems on the cloud), anti-malware systems (strategically placed, continually updated), media management (using encryption; degaussers for erasing).

(4) *Key operational practices*.[345] Other key operational practices required in the cloud will include archival, backup, and recovery procedures (well documented processes); incident management (integrating people, processes and technologies), problem management (handling defects), change management (utilizing a configuration control board), configuration management (with guides and standards for each operating system/application within the cloud), patch management (involving security and system administrators), security audits and reviews (third party verified security compliance).

---

[342] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

[343] Ibid.

[344] Ibid., 561.

[345] Tipton, *Official (ISC)2 Guide to the CISSP CBK*.

Conclusions. This section specifically addressed patching; logging, monitoring and auditing; and the malicious insider. Following, general OPSEC practices for cloud were provided. This domain requires attention to detail in the daily tasks that involve securing the cloud in order to protect DoD assets. Since the DoD could be hiring a cloud provider to provide a private solution, the responsibilities for ensuring operational security require continued dialogue and partnership.

8. Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)

The emphasis of this domain is to ensure continuous service without external or internal interruptions. Since the DoD conducts many mission critical operations, the reliability of the cloud solution is of paramount significance. This domain addresses threats and countermeasures associated with an external provider terminating business; cloud outages, data loss and latency; and cloud provider lock-in.

Vendor terminates business without sufficient notice. The availability of data is at risk if a provider terminates business without sufficient notice for transition or retrieval of data.[346] Such situations may impact secure operations of a business, as evident in 2008 when an external cloud vendor named Linkup terminated operations with little notice to 20,000 customers.[347] This incident resulted in negative repercussions; for one CEO, only 55 percent of company data was saved, while the status of the rest was questionable.[348]

Cloud outages, data loss, and latency pose threats to cloud availability. Environmental factors (i.e., hurricane causes power outage), technical failures, malicious threats, malware, and user error can lead to cloud outages and lost data. Resource overloading or denial of service conditions within a shared cloud environment could

[346] Scott Paquette, Paul T. Jaeger, and Susan C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," *Government Information Quarterly*, Vol. 27, Issue 3 (July 2010).

[347] Ibid.

[348] Ibid.

impair availability for all users of the shared resources.[349] Latency problems can also arise in clouds, for example, as a result of the distance between a user's applications and data on the cloud or as a result of slow encryption services.[350]

Lock-in with one provider (loss of interoperability and business continuity). "Lock-in" is a major hindrance to "data, application and service portability."[351] Due to a lack of standards with cloud, customers may become "locked in" to one provider and unable to move data from cloud to cloud.[352] This is common, as mentioned in the application security domain, among APIs (they are proprietary instead of standardized); since many APIs are not publicly available, it is difficult to create interoperability among multiple venders.[353] The problem of lock-in can become particularly serious if a provider goes out of business, leaving the customer not only without a provider, but also without a means of porting data to a new provider.

Some preventative measures to this domain include:[354]

- Inspect and engage with provider on their BCP and DRP. Both plans should map to recognized standards, i.e., BS 25999; reviewed, exercised and validated periodically; and actively supported by management.[355]
- Request back-up copies of data once a month from providers; this is excellent in case of environmental failure or cloud provider going out of business.[356]

---

349 Perry, "Security for Cloud Computing."

350 Claburn, "Google Plans Private Government Cloud."

351 Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," European Network and Information Security Agency, November 2009, at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (accessed August 6, 2010), 9.

352 Ibid.

353 Scott Paquette, Paul T. Jaeger, and Susan C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, Vol. 27, Issue 3 (July 2010)

354 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 50.

355 Ibid., 51.

356 Cyril Onwubiko, "Security Issues to Cloud Computing," *Computer Communications Networks: Cloud Computing Principles, Systems and Applications,* (London: Springer, 2010).

- When selecting encryption services, balance objectives with confidentiality and security with those for performance and availability.[357]
- Define and ensure cloud provider understands DoD recovery time objectives (RTOs); verify "technology roadmaps, policies, and operational capabilities" supporting these requirements.[358]
- Ensure questions about availability are raised with the cloud provider, i.e., "what happens to your organization's applications and data in the event that the provider goes out of business?[359] The BCP/DCP should cover these questions.
- Ensure "scheduled data backup and safe storage of …backup media" can provide a minimum level of availability. [360]
- Ensure a cloud provider gives priorities to cloud instances for availability and appropriate resource utilization.[361]
- Ensure a cloud provider takes measures to ensure reliability, for example, by executing "applications across multiple physical servers."[362]
- Ensure a provider's BCP and DRP includes an integration strategy for portability of data, in which partnerships with diverse technology vendors allow synchronization and business continuity.[363]

Conclusions. Since the terrorist attacks since 9/11, the private sector plans for recovery during emergencies and maintaining business continuity as stipulated by Title IX, "9/11 Commission Recommendation Act of 2007."[364] Since mission-critical operations are ongoing during war, the DoD should stipulate appropriate standards to protect the availability of data directly supporting mission-related functions. The

357 Dr. Dobb, "Six Steps to Securing Cloud Computing," Security Dark Reading, March 10, 2010, at: http://www.darkreading.com/security/app-security/showArticle.jhtml?articleID=223400093&cid=RSSfeed (accessed July 10, 2010).

358 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," p. 50.

359 Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

360 Harauz, "Data Security in the World of Cloud Computing," 62.

361 Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud," Computer Communications and Networks: Cloud Computing Principles, Systems and Applications, (London: Springer, 2010), 7.

362 Ibid., 7.

363 Linthicum, "The top five mistakes cloud venders make –and you should watch for."

364 Tipton, Official (ISC)2 Guide to the CISSP CBK, 268.

standards can be verified through a validated and exercised BCP and DRP developed by the DoD and any third party provider, as supported by senior management.

9. Legal Regulations, Compliance and Investigation

The legal regulation, compliance and investigation domain specifically addresses SLAs, blurred responsibilities between providers and customers, the need for incident handling processes, compliance with legal regulations, intellectual property and privacy, cloud employee monitoring and surveillance, the utility of cloud security experts, and the highlighted significance of IT and legal personnel working together in formulation of the SLA or contract.

Problems associated with SLAs. In a recent study by Yankee Group on 41 cloud computing companies, researchers found that "cloud vendors offer poor service guarantees and limited financial redress if their service fails," while "[g]et-out clauses are rife, and robust privacy policies are rare."[365] In Yankee Group's study, only half of the 41 cloud companies offered SLAs, and none of the 41 companies provided financial reparations for data loss.[366]

The DoD must ensure that SLAs with cloud computing providers are clear, meticulous, meaningful, and comprehensive. Typically, an SLA stipulates timelines for fixing problems (availability), but the DoD must ensure it also protects confidentially and integrity. The following are examples of questions that should be answered in a few of the domains:

- *Physical and environmental security:* Where is the data physically being stored (i.e., allied countries with privacy laws appropriate to protection from disclosure)? Is the computer center and building infrastructure in compliance with physical security standards/regulations? What provisions

[365] Microsoft, "Snapshot Full Strategic Report," at: http://download.101com.com/GIG/Custom/Microsoft/SnapCloudFinal.pdf (accessed September 1, 2010).

[366] Ibid.

are made for environmental/natural (i.e., fire, heat), man-made (i.e., access control to areas/buildings), and political threats or disasters affecting physical security of data location?[367]

- *Business continuity/disaster recovery:* What preventative measures does the cloud provider use (i.e., backups, redundancies) to ensure data is continually available?
- *Legal, regulation, investigation and compliance:* "Does the cloud provider meet legal and regulatory requirements?[368] Will a cloud provider give timely assistance to meet investigative/audit requirements?
- *Telecommunications and network security:* Will a cloud provider isolate data properly? How will a cloud provider protect infrastructure, platform and software from hacking?
- *Information security governance and risk management:* Will the cloud provider's security policies and contract align with DoD regulations?[369] Does the SLA incorporate requirements of the customer's risk management plan to protect the CIA of the data?[370]

Blurred responsibility between customer and external or third party cloud computing provider creates security vulnerabilities for exploitation. The legal issue of responsibility is a problem with providers; for instance, where are the lines of delineation between the cloud storage provider or the entity leasing storage for its applications and data?[371] Most CIOs voice concerns over security with cloud computing due to movement of the trust boundary (delineation of security responsibilities) that exists between a provider and the customer.[372] CSA purports that in many cases with IaaS and PaaS, much of "orchestration, configuration and software development" is conducted by

---

[367] Justin Kallhoff, "Physical Security Threats," *Global Information Assurance Certification Organization,* March 30, 2007, at: http://www.giac.org/resources/whitepaper/physical/287.php (accessed July 9, 2010), 1.

[368] Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

[369] Barbara DePompa, "The Cloud's Standard Imperative."

[370] Paquette, Jaeger, and Wilson, "Identifying the security risks associated with governmental use of cloud computing."

[371] Harauz, "Data Security in the World of Cloud Computing," 62.

[372] Tim Mather, Subra Kumaraswamy, and Shahed Latif, *Cloud Security and Privacy*, (Sebastopol: O'Reilly Media, Inc., 2009).

the customer that responsibility stays with the customer.[373] These lines of responsibility require accountability and clarification.

A security model must be developed to promote CIA. Aspects of this model need to be scrutinized, outlined and verified in minute details of an SLA. Providers and customers must be cognizant of responsibilities within virtual environments.[374] Cloud customers need to understand system management process for access control, change management, and vulnerability management, as well as patching and configuration management.[375] Some providers today create and utilize dashboards to increase visibility and remove guesswork in the service instrumentation/metrics between provider and customer.[376]

Problems with incident response. Security incidents are defined as "any real or suspected adverse event in relation to the security of computer systems or computer networks" or "the act of violating an explicit or implied security policy."[377] Incident reporting is often negatively affected by concerns over confidentiality.[378] Security incidents can occur: (1) when a vulnerable application is uploaded or deployed to a cloud environment; (2) as a result of inherent architectural flaws, (3) from discrepancies in hardening processes, or (4) from a miscellaneous user oversight.[379] Incident handling will differ based on data location, but a process for handling incidents must be in place.

---

[373] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 35.

[374] Mather, Kumaraswamy, and Latif, *Cloud Security and Privacy*.

[375] Ibid.

[376] Ibid.

[377] CERT Coordination Center, Carnegie Mellon University Software Engineering Institute, at: http://www.cert.org/csirts/csirt_faq.html#2 (accessed September 1, 2010).

[378] Harauz, "Data Security in the World of Cloud Computing," 62.

[379] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 54–55.

Several strategies for incident handling include:

- Define what constitutes an incident (i.e., data breach) and events (i.e., suspicious IDS alerts) to a provider before using services.[380]
- Verify a cloud provider's incident response program and notification chain.[381]
- Verify the cloud provider's detection/analysis tools comply with DoD instructions.[382]
- Log, report and investigate security incidents at the hypervisor level.[383]
- Since cloud computing uses virtual servers, define methods of evidence collection in advance.[384] If a VM is powered down, the host operating system can still access the disk image; this allows tampering of potential forensic data.[385]

Compliance deficiencies. Providers need to comply with information system security requirements whether internal DoD policy, ISO policies or certification and accreditation processes. Without attention to security compliance, the CIA of data could become easily compromised. In a study done by security analysts, gaps in compliance with ISO 27002 were discovered in cloud computing; following, these analysts recommended twenty mitigating security strategies that are dispersed throughout this thesis.[386]

Several strategies to mitigate compliance deficiencies include:

- An SLA with an external provider can stipulate security standards, certification/accreditation, and regulatory requirements. Many of these general standards were covered under governance in this thesis. Many are yet to be developed.

---

[380] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 54–55.

[381] Ibid.

[382] Ibid.

[383] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[384] Ibid.

[385] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[386] Ibid.

- For management of information security systems, providers must comply with ISO/IEC 27001/27002, and achieve ISO/IEC 27001 certification.[387] Providers must verify compliance with evidence via audit logs, change management paperwork, and test procedure reports.[388]
- Providers should allow auditing by the customer for verification purposes.[389] Providers/customers should comply with SAS 70 Type II for auditing requirements.[390]
- "Standard procedures, tools, [and] data formats" should be incorporated within industry as developed.[391]
- Providers/customers should verify new instances on a cloud comply with "defined, tested and approved specifications."[392]

"Google Apps for Government" is "the first suite of cloud applications to meet Federal Information Security Management Act (FISMA) certification and accreditation for the U.S. government."[393]

Intellectual property and privacy. In the context of information system security, this domain also covers protection of intellectual property (from copy or use without compensation to the owner), and privacy (the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information).[394] In cloud computing, these same laws (copyright, patent, trademark, trade secret, licensing issues) apply, and thus, technical, administrative, and policy controls unique to cloud computing must establish appropriate protections. A customer

---

[387] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 38.

[388] Ibid.

[389] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security."

[390] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 38.

[391] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security."

[392] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud," 7.

[393] David Linthicum, "Google removes cloud security barrier for the government," *InfoWorld*, July 28, 2010, at: http://www.infoworld.com/d/cloud-computing/google-removes-cloud-security-barrier-the-government-889 (accessed September 10, 2010).

[394] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 514.

must retain ownership of its information in the "original and authenticable format."[395] Privacy laws vary based on jurisdiction, yet OECD establishes generic principles and recommendations from which cloud security legislation can develop.

Employee monitoring. Another significant issue in this domain is employee monitoring and surveillance.[396] The levels of third party providers in a cloud computing environment quickly spiral out of a customer's control, and the time required to verify a provider is self-monitoring its employees becomes an afterthought. Stipulating that a cloud provider and third parties require employee-signed "acceptable use policies" could assist in prevention of employee abuse, while monitoring could deter the same employee misuse.[397] This control assists in maintaining cloud computing employee productivity and efficiency, reducing security incidents, and controlling for the insider threat.[398]

Liability with due care and diligence. The issue of monitoring employees sheds light on liability. Within the DoD, corporate assets in a cloud solution may be handled by a third party cloud provider; in this case, due care and due diligence of proper protections is paramount. For instance, if a cloud provider does not meet regulatory requirements in the percentage of an IT budget devoted to security, he could be held liable to legal repercussions.[399] An SLA will require legal reviews to verify that regulatory requirements are specific enough to establish and enforce due care and diligence.

Incidents, forensics, and a cloud security expert. It is important to establish incident response processes, procedures and policy within a cloud computing solution. In addition, staff positions in cloud security should be established within organizational and national-level CERTs. Without a cloud expert, the phases of triage, investigation, containment, analysis and tracking; recovery and repair; and debrief/feedback within a

---

[395] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 36.

[396] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 516.

[397] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 516–517.

[398] Ibid.

[399] Ibid.

cloud computing incident response will be more difficult.[400] Technical forensics for crime investigation and incident response in a cloud environment will require tailored approaches, specifically with isolation and containment of data. Such cloud security experts on an IT organizational staff, positioned within the Information Assurance section, could assist with clarifying responsibilities of a customer verse provider in incident response, forensic investigation, and daily security maintenance.

Conclusions. Legal considerations are prolific and span the scope of the ten domains. Once a customer decides upon a provider, the SLA will be the key to negotiating and outlining provisions from pre-contract, contract term, post-contract monitoring, and termination.[401] Due to technical nuances of cloud computing, it is recommended that legal staff work closely with a customer's cloud security expert in the negotiation.[402] There is a lack of precedence in legal issues within cloud computing from which to build, especially in digital evidence, which makes this domain more challenging.[403] Other challenges include holding a third party responsible. This is addressed using similar methodologies (legal contracts/SLAs) as incorporated in past government situations for contract services. Cloud computing is a new arena for efficiency and monetary gains, and requires addressing appropriate legal issues in advance, in order to prove viable and useful for furthering missions leading to success in the DoD.

10. Physical and Environmental Security

Physical and environmental security for cloud computing presents threats in several areas: data location, audit transparency, facility/server room security, server isolation, data deletion, tempest and proper separation. This chapter addresses these threats and associated countermeasures.

---

[400] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 516–517.

[401] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 36.

[402] Ibid., 35.

[403] Ibid., 35.

Data location could lead to compromise. If DoD data is stored in a foreign country, the government of that country could potentially seize equipment holding the data. This might happen, for example, if DoD data is stored on a device that also holds the data of a criminal enterprise that the government is investigating.

To mitigate this risk, SLAs should stipulate where data may be stored and how it is to be protected during a criminal investigation. A cloud provider for the DoD should "commit to storing and processing data in specific jurisdictions," and "obey local privacy requirements"[404] in a manner equivalent to DoD-level guardianship.[405] This requirement is also backed by U.S. privacy laws, such as the U.S. Safe Harbor program, which mandates knowledge of data storage location at all times.[406] This law encourages providers to stay within legal jurisdiction and decrease security risks.[407]

Lack of transparency/openness to audit. Customer auditing plays an important role in assuring that proper security standards are met, including standards for physical security. Since some providers may not allow auditing, the DoD should only use providers that do. A cloud provider's security posture (including physical/environmental controls/personnel hiring practices/privacy controls over data) must be transparent[408] and accountable to the DoD, and thus open to inspection/audit, and documented in an SLA.[409]

404 Brodkin, "Gartner: Seven cloud-computing security risks," 1.

405 Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," 36.

406 Mather, Kumaraswamy, and Latif, *Cloud Security and Privacy*.

407 Ibid.

408 Bret Michael, "In Clouds Shall We Trust?" *IEEE*, Vol. 7, Issue 5 (Sept - Oct 2009), 3.

409 McDaniel and Smith, "Outlook: Cloudy with a Chance of Security Challenges and Improvements," 79.

An audit should include the following actions relating to physical security:

- Perform onsite inspections of cloud facilities on a periodic basis.[410]
- Identify physical interdependencies within a provider's infrastructure.[411] Verify a cloud provider demonstrates "comprehensive compartmentalization of systems, networks, management, provisioning, and personnel."[412]
- Ensure uninterruptible power supply systems are in place for continuity of power and continuous operations.[413]
- Inspect documentation of internal/external security controls to validate compliance with industry standards.[414]

Improper facility physical security/environmental controls. The CIA of DoD data could become compromised if a building were to collapse for any reason, due to an environmental issue or non-compliance with building codes. In June 2009, Amazon.com's EC2 data center experienced repercussions of a lightning strike, which resulted in a four hour outage.[415] Facility construction considerations/requirements (roads, barriers, doors, locks, safes, windows, lighting, and crime prevention through environmental design) must be based on a defense in depth approach and in compliance with DoD physical security standards.[416] Environmental protection/controls (fire, power; heating, ventilation, and air-conditioning (HVAC), water) should be in place with appropriate alarms.[417]

---

[410] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 50.

[411] Ibid.

[412] Ibid., 53.

[413] Tipton, *Official (ISC)2Guide to the CISSP CBK*.

[414] Brunette and Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1," 50.

[415] Paquette, Jaeger, and Wilson, "Identifying the security risks associated with governmental use of cloud computing," 245–253.

[416] Tipton, *Official (ISC)2 Guide to the CISSP CBK*,579–665.

[417] Ibid., 656–662.

Lack of proper security in the server room.[418] The server rooms used by cloud providers may be vulnerable to natural disasters and intentional acts of "sabotage, espionage and data theft."[419] DoD customers must make sure that their providers employ adequate server room security, to include: a single controlled entry/exit, rack locks, dielectric fiber cabling or optical isolators (lightning protection), back-up generators (power failure prevention), proper HVAC, and least privilege or need-to-know access control.[420]

"*Insecure or incomplete data deletion/data persistence*."[421] Compromise becomes commonplace when media controls/destruction processes are not in place. When requested by the DoD, an external cloud provider must destroy or remove data and render it unrecoverable from the cloud or an external device.[422] In some cases, data remnants can only be removed via physical destruction. Customers must verify a cloud provider records current and past records (throughout full lifecycle) for removal of physical and virtual instances.[423]

Improper tempest/shielding. Emanations from computer equipment can reveal sensitive data. To mitigate this risk, cloud providers should shield buildings, computers, wireless antennae, cables, keyboards and screens.[424] In some cases, DoD surveillance and tempest technologies might provide better protection than commercial, in which case, private clouds using these resources might be preferable to a public cloud.

Lack of isolation/segregation. Without physical separation in a multi-tenant environment, the traversal vulnerability can compromise data from a VM sharing the

---

[418] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 647–652.

[419] Ibid., 650.

[420] Ibid., 579–675.

[421] Catteddu and Hogben, "Cloud Computing: Benefits, Risks, and Recommendations for Information Security," 10.

[422] Ibid., 41.

[423] Durbano, Rustvold, Saylor and Studarus, "Securing the Cloud."

[424] Tipton, *Official (ISC)2 Guide to the CISSP CBK*, 141–142.

same VM or physical server. Cloud customers should verify that the physical machine holding their data, if shared with other users, contains access controls to prohibit interference, whether intentional or malicious.[425]

Conclusions. The physical domain circa cloud computing presents several opportunities for compromise without sound security implementations. Physical compartmentalization within a virtual and multi-tenant environment is one safeguard that mitigates the risk of a malicious attacker exploiting the hypervisor vulnerability. Other safeguards include physically securing facility and equipment with controls to prevent unauthorized access to valuable data.

[425] Pelgrin, "Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter."

VI. CONCLUSION

The ten domains provide a credentialed standard of security to protect the CIA of cloud computing.

- The access control domain addressed countermeasures for frictionless registration, account hijacking, and authentication attacks such as strong or multi-factor authentication. Recommendations were provided for overarching identity and access management issues, specifically involving identity provisioning, authentication, federation, authorization and user profile management. Lastly, generic countermeasures were discussed, such as integration of access control with the DoD common access card, SAML, WS-federation, and proactive auditing and monitoring.
- The telecommunication and network security domain addressed the relevant issues and countermeasures to cloud hacking and to DoS and VM attacks. Boundary protection is paramount both within and outside of the cloud, and the provider must ensure that provisions protect the CIA of a customer's data. Some of these measures include internal/external layered security controls such as IDS & IPS, as well as compartmentalization of virtual instances in order to protect dispersive system components.
- The security architecture and design domain dissected several important areas: establishing isolation management within shared technologies; designing architectures for meeting customer demands for service and availability; and certifying and accrediting systems before use, while leveraging federal solutions.
- The application security domain addressed exploitation and countermeasures to protect insecure interfaces. It provided methods on increasing security for PaaS, SaaS, and IaaS in the realm of message

communication, information handling, key management, SDLC, tools and services, metrics, economics, and inter-host communication.

- The cryptographic domain highlighted that traditional encryption processes can transfer to the cloud, while encouraging encryption in transit, at rest and for backup purpose; and noted the potential use of homomorphic encryption techniques to secure confidentiality in the future.
- The security architecture and design domain discussed establishing isolation management within shared technologies; designing architectures for meeting service and availability demands; and certifying and accrediting systems and leveraging federal solutions.
- The OPSEC domain highlighted the importance of patching; logging, monitoring and audit; and personnel practices to protect against the malicious insider.
- The BCP and DRP domain addressed the importance of ensuring the availability of data that is needed for mission-related functions. BCPs and DRPs must be validated and exercised by the DoD and any third party provider.
- The legal regulation, compliance and investigation domain specifically addressed SLAs, blurred responsibilities between providers and customers, the need for incident handling processes, compliance with legal regulations, intellectual property and privacy, cloud employee monitoring and surveillance, and the need for cloud experts. It highlighted the significance of IT and legal personnel working together in formulation of the SLA or contract.
- The physical and environmental security domain identified threats and countermeasures in several areas: data location, audit transparency, facility/server room security, server isolation, data deletion, tempest and proper separation.

Through use of the ten domains, the DoD can better mitigate threats that are inherent in this new cutting edge technology. By taking precautions with the new technology of cloud computing, the DoD can reap benefits in efficiency while ensuring the CIA of their data remains intact.

Recommendations for future research include readdressing this thesis in five years when cloud computing technology has matured. Any of the ten domains could easily provide fodder for a thesis in the future as well.

LIST OF REFERENCES

Arnold, John. "Domain 10: Guidance for Application Security V2.1." *Cloud Security Alliance*, July 2010, at: http://www.cloudsecurityalliance.org/guidance/csaguide-dom10-v2.10.pdf (accessed August 21, 2010).

Badger, Lee, and Tim Grance. "Standards Acceleration to Jumpstart Adoption of Cloud Computing." *NIST Computer Security Division Briefing*, May 20, 2010, at: http://www.slideshare.net/kvjacksn/nist-cloud-computingforumbadgergrance (accessed November 24, 2010).

Baldor, Lolita C. "Pentagon spends $100M to fix Cyber Attacks." *Physorg.com*, April 7, 2009, at: http://www.physorg.com/news158333019.html (accessed May 17, 2010).

Beckman, Mel. "Cloud Options that IT will Love." *An Interactive eBook: Cloud Computing*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

Biscotti, Fabrizio, Benoit J. Lheureux, Andrew Frank, Jeffrey Roster, Susan Cournoyer, and Venecia K. Liu. "Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014." *Gartner, Inc*., June 2, 2010, at: http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1378513 (accessed October 23, 2010).

Bolin, Jason S. *Use Case Analysis for Adopting Cloud Computing in Army Test and Evaluation.* Naval Postgraduate School Master's Thesis, September 2010, at: http://edocs.nps.edu/npspubs/scholarly/theses/2010/Sep/10Sep_Bolin.pdf (accessed October 24, 2010).

Brodkin, Jon. "Gartner: Seven cloud computing security risks." *Infoworld*, July 2, 2008, at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0 (accessed November 6, 2010).

Brunette, Glenn and Rich Mogull, "Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1." *Cloud Security Alliance*, December 2009, at: http://www.cloudsecurityalliance.org/csaguide.pdf (accessed July 20, 2010).

Carey, Allan. "Cloud Assurance Still Missing," *Information Assurance Newsletter*, Vol. 13, No. 1 (Winter 2010).

Catteddu, Daniele, and Giles Hogben, eds. “Cloud Computing: Benefits, Risks, and Recommendations for Information Security.” *European Network and Information Security Agency*, November 2009, at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment (accessed August 6, 2010).

CBS Interactive Staff, “DoD Gates: We’re always under cyberattack,” *ZDNet*, April 22, 2009, at: http://www.zdnet.com/news/dod-gates-were-always-under-cyberattack/290770 (accessed May 17, 2010).

Chabrow, Eric. “Balancing Act: Security Meets Functionality.” *Government Information Security Articles*, December 14, 2009, at http://www.govinfosecurity.com/articles.php?art_id=2005 (accessed May 17, 2010).

Chabrow, Eric. “Can Cloud Be More Secure Than Legacy Systems?” *Government Information Security Articles*, July 1, 2010, at: http://www.govinfosecurity.com/articles.php?art_id=2714&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GovinfosecuritycomRssMain+%28GovInfoSecurity.com+RSS+Main%29 (accessed September 10, 2010).

Chabrow, Eric. “White House Issues Secure Cloud Computing Guidance: FedRAMP Requirements aimed to easy cloud computing adoption,” *Government Information Security Articles*, November 2, 2010, at: http://www.govinfosecurity.com/articles.php?art_id=3063 (accessed November 6, 2010).

Chart by Deputy Assistant Secretary of Defense, “*Cyber, Identity & Information Assurance (CIIA) Related Policies and Issuances: Build and Operate a Trusted GIG*,” July 30, 2010, at: http://iac.dtic.mil/iatac/download/ia_policychart.pdf (accessed September 10, 2010).

Chrisholm, Theo. “U.S. Air Force Selects IBM to Design and Demonstrate Mission-oriented Cloud Architecture for Cyber Security.” *IBM Press Room*, February 4, 2010, at: http://www-03.ibm.com/press/us/en/pressrelease/29326.wss#release (accessed November 1, 2010).

Cachin, Christian, Idit Keidar, and Alexander Shraer. “Trusting the Cloud.” *ACM SIGACT News*, 2009.

Claburn, Thomas. “Google Plans Private Government Cloud.” *Information Week Government*, September 16, 2009, at: http://www.informationweek.com/news/government/cloud-saas/showArticle.jhtml?articleID=220000732&pgno=1&queryText=&isPrev (accessed August 11, 2010).

Defense Market. “DoD Embraces Cloud Computing.” *Defense Market Research and Analysis.* October 29, 2010, at: http://www.defensemarket.com/?p=67 (accessed May 2010, 31).

DePompa, Barbara. “The Cloud’s Standard Imperative.” *Defense Systems: Knowledge Technologies and Net-Centric Warfare*, May 5, 2010, at: http://defensesystems.com/microsites/2010/cloud-computing/cloud-standards-imperative.aspx (accessed May 29, 2010).

DoD 8570.01-M, “*IA Workforce Improvement Program.*” May 15, 2008, at: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (accessed May 27, 2010).

Durbano, James P., Derek Rustvold, George Saylor and John Studarus, “Securing the Cloud.” *Computer Communications and Networks: Cloud Computing Principles, Systems and Applications*, London: Springer, 2010.

Eagle, Liam. “DDoS Attack Hits Amazon Cloud Customer Hard.” *Web Host Industry Review*, October 6, 2009, at: http://www.thewhir.com/web-hosting-news/100609_Outage_Hits_Amazon_Cloud_Customer_Hard (accessed August 16, 2010).

Fried, Ina. “Software Outage Casts Cloud Over Microsoft.” *CNET News*, October 10, 2009, at: http://news.cnet.com/8301-13860_3-10372525-56.html (accessed June 14, 2010).

Genova, Windsor. “Cloud Software Vulnerable to Hackers, Defcon Survey Says.” *International Business Times*, August 25, 2010, at: http://www.net-security.org/secworld.php?id=9773 (accessed September 10, 2010).

Gregg, Michael. “Ten Security Concerns for Cloud Computing.” *Global Knowledge Training, LLC: Expert Reference Series of White Papers*, 2010, at: http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_VI_10SecurityConcernsCloudComputing.pdf (accessed July 31, 2010).

Halbheer, Roger. “Moving to the Cloud in an Azure Sky: A Security Review.” *Power point briefing by Microsoft Corporation*, at: http://halbheer.info/security (accessed Aug 3, 2010).

Harauz, John, Lori M. Kaufman, and Bruce Potter. “Data Security in the World of Cloud Computing,” *IEEE Security & Privacy*, July/Aug 2009, at: http://www.idi.ntnu.no/emner/tdt60/papers/05189563.pdf (accessed November 24, 2010).

Harris, Shon. *All-in-one CISSP Exam Guide.* New York: McGraw Hill, 2010.

———. *All-in-one CISSP Exam Guide*. New York: McGraw Hill, 2008.

Hasan, Ragib. “Security and Privacy in Cloud Computing.” *John Hopkins University Lecture Slides*, February 1, 2010, at: http://www.cs.jhu.edu/~ragib/sp10/cs412/lectures/600.412.lecture02.pdf (accessed September 10, 2010).

Help Net Security Website. “*Cloud Computing: Risks Outweigh the Benefits.*” March 23, 2010, at: http://www.net-security.org/secworld.php?id=9051 (accessed September 10, 2010).

Higgins, John K. “Uncle Sam Wants the Cloud, Part 1.” *E-Commerce Times*, September 29, 2010, at: http://www.ecommercetimes.com/story/70924.html (accessed October 24, 2010).

Hogben, Giles. “ENISA Clears the Fog on Cloud Computing Security.” *European Network and Information Security Agency*, November 20, 2009, at: http://www.enisa.europa.eu/media/press-releases/enisa-clears-the-fog-on-cloud-computing-security-1/?searchterm=cloud%20security (accessed September 10, 2010).

Hoover, J. Nicholas. “Army Consolidates Email Under DISA Cloud.” *Information Week Government*, October 26, 2010, at: http://www.informationweek.com/news/government/enterprise-apps/showArticle.jhtml?articleID=227900731&queryText=cloud%20security (accessed October 31, 2010).

Hubbard, Dan, and Michael Sutton, “Top Threats to Cloud Computing, V1.0.” *Cloud Security Alliance*, March 2010, at: http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (accessed July 20, 2010).

Jackson, Kevin. “CANES and the Cloud.” *Military Information Technology*, December 2009, at: http://www.military-information-technology.com/mit-archives/219-mit-2009-volume-13-issue-11/2353-canes-and-the-cloud.html (accessed November 6, 2010), Vol. 13, Issue 11.

Kallhoff, Justin. “Physical Security Threats.” *Global Information Assurance Certification Organization*, March 30, 2007, at: http://www.giac.org/resources/whitepaper/physical/287.php (accessed July 9, 2010).

Katzman, Joseph, and Fred Donovan. “Head in the Clouds: DoD Turns to Cloud Computing.” *Defense Industry Daily*, May 25, 2010, at: http://www.defenseindustrydaily.com/defense-cloud-computing-06387/ (accessed May 29, 2010).

Kay, Russell. “An Interactive eBook: Cloud Computing,” *Custom Publishing Groups*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

Knies, Rob. “Peering into Future of Cloud Computing.” *Microsoft Research*, February 24, 2009, at: http://research.microsoft.com/en-us/news/features/ccf-022409.aspx (accessed October 23, 2010).

Krebs, Brian. “Obama: Cyber security is a National Security Priority.” *The Washington Post*, May 29, 2009, at: http://voices.washingtonpost.com/securityfix/2009/05/obama_cybersecurity_is_a_natio.html (accessed Jun 13, 2010).

Kubic, Chris. “DoD Cloud Computing Security Challenges.” *Briefing by Chief Architect, Information Assurance Architecture and Systems Security Engineering Group, National Security Agency*, at: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/cloud-computing-IA-challenges_ISPAB-Dec2008_C-Kubic.pdf (November 6, 2010).

Kumar, Karthik, and Yung-Hsiang Lu. “Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?” *Computer*, Vol. 44, No. 4 (April 2010).

Kundra, Vivek. “Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, Draft Version 0.96.” *CIO Council*, November 2, 2010, at https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf (accessed November 24, 2010).

———. “Public Sector Cloud Computing Case Study: Army Experience Center,” *CIO.gov*, June 8, 2010, at: http://cio.gov/pages.cfm/page/Public-Sector-Cloud-Computing-Case-Study-Army-Experience-Center (accessed October 27, 2010).

———. “State of Public Sector Cloud Computing.” *CIO.gov*, May 20, 2010, at: http://www.cio.gov/pages.cfm/page/STate-of-Public-Sector-Cloud-Computing (accessed November 24, 2010).

Lentz, Robert F. “Statement before the U.S. House of Representatives Armed Services Committee Subcommittee on Terrorism, Unconventional Threats and Capabilities,” May 5, 2009, at: http://armedservices.house.gov/pdfs/TUTC050509/Lentz_Testimony050509.pdf (accessed November 24, 2010).

Linthicum, David. “Three Cloud Computing Mistakes You Can Avoid Today.” *MISAsia*, March 12, 2010, at: http://mis-asia.com/cio_focus/technology/3-cloud-computing-mistakes-you-can-avoid-today (accessed September 10, 2010).

———. “Google removes cloud security barrier for the government.” *InfoWorld*, July 28, 2010, at: http://www.infoworld.com/d/cloud-computing/google-removes-cloud-security-barrier-the-government-889 (accessed September 10, 2010).

Mell, Peter and Tim Grance, “Effectively and Securely Using the Cloud Computing Paradigm.” *National Institute for Standards and Technology, IT Laboratory*, October 7, 2009, at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010).

Messmer, Ellen. “US military takes cloud computing to Afghanistan.” *Network World*, September 23, 2010, at: http://www.networkworld.com/news/2010/092310-cloud-computing-afghanistan.html?page=1 (accessed October 1, 2010).

Michael, Bret, and George Dinolt. “Establishing Trust in Cloud Computing.” *Information Assurance (IA) Newsletter*. Vol. 13, No. 2 (Spring 2010).

———. “In Clouds Shall We Trust?” *IEEE*, Vol. 7, Issue 5 (Sept - Oct 2009).

Microsoft, “Snapshot Full Strategic Report,” at: http://download.101com.com/GIG/Custom/Microsoft/SnapCloudFinal.pdf (accessed September 1, 2010).

Mills, Elinor. “Pentagon Spends Over $100 million on Cyberattack Cleanup.” *CNET News*, April 7, 2009, at: http://news.cnet.com/8301-1009_3-10214416-83.html (accessed May 17 , 2010).

———. “Twitter, Facebook Attack Targeted One User.” *Cnet News*, August 6, 2009, at: http://news.cnet.com/8301-27080_3-10305200-245.html (accessed September 10, 2010).

National Institute for Standards and Technology Website, Computer Security Division: Computer Security Resource Center, May 11, 2009, at: http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed September 10, 2010).

Naxal Watch, "U.S.: DoD Advances Cloud Computing Usage." *Intellibriefs*, January 12, 2010, at: http://intellibriefs.blogspot.com/2010/01/us-dod-advances-cloud-computing-usage.html (accessed October 1, 2010).

Newton, Ben. "Building Private and Community Clouds for the DoD." *Defense Systems*, September 23, 2010, at: http://defensesystems.com/Articles/2010/09/02/Industry-Perspective-Automating-the-Cloud.aspx?Page=2 (accessed October 1, 2010).

Owens, Dustin. "Securing Elasticity in the Cloud." *Association for Computing Machinery*, May 6, 2010, at: http://queue.acm.org/detail.cfm?id=1794516 (accessed September 10, 2010).

Paquette, Scott, and Paul T. Jaeger, and Susan C. Wilson. "Identifying the security risks associated with governmental use of cloud computing." *Government Information Quarterly*, Vol. 27, Issue 3 (July 2010).

Paul, Frederick. "Cloud Computing's Dirty Little Secret." *Enterprise Efficiency*, August 30, 2010, at: http://www.enterpriseefficiency.com/author.asp?section_id=898&doc_id=196259 (accessed October 2, 2010).

Pelgrin, William F. "*Multi-State Information Sharing & Analysis Center (MS-ISAC) Monthly Security Tips Newsletter*." April 2010, at: http://www.msisac.org/awareness/news/2010-04.cfm (accessed July 26, 2010).

Perry, Christopher. "Security for Cloud Computing." *Department of the Navy Chief Information Officer Website*, May 18, 2010, at: http://www.doncio.navy.mil/ContentView.aspx?ID=1744 (accessed August 27, 2010).

Pettey, Christy, and Ben Tudor. "Gartner Says Worldwide Cloud Services Market to Surpass $68B in 2010." *Gartner Newsroom*, June 22, 2010, at: http://www.gartner.com/it/page.jsp?id=1389313 (accessed October 23, 2010).

Pokharel, Manish, and Jong Sou Park. "Cloud Computing: Future solution for e-Governance." *ACM International Conference Proceeding Series*, Vol. 322, (New York: ACM, 2010).

Prince, Brian. “IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering.” *E-Week.com*, June 25, 2009, at: http://www.eweek.com/c/a/Security/IBM-Uncovers-Encryption-Scheme-That-Could-Improve-Cloud-Security-Spam-Filtering-135413/ (accessed November 24, 2010).

Ramienski, Dorothy. “DoD IT experts open up about cloud deployment.” *Federal Executive Forum*, November 10, 2009, at: http://www.federalnewsradio.com/index.php?nid=35&sid=1808816 (accessed August 11, 2010).

Rigby, Bill. “An Interactive eBook: Cloud Computing.” *Computer World*, July 15, 2010, at: http://www.networkworld.com/whitepapers/nww/pdf/eGuide_cloud_5brand_final.pdf (accessed July 15, 2010).

Sims, Jennifer E., and Burton Gerber. *Transforming U.S. Intelligence.* Washington, D.C.: Georgetown University Press, 2005.

Sutter, John D. “Twitter hack raises questions about ‘cloud computing.’ *CNN.com*, July 16, 2009, at: http://www.cnn.com/2009/TECH/07/16/twitter.hack/index.html (accessed July 13, 2010).

Tipton, Harold F. *Official (ISC)2 Guide to the CISSP CBK*. Boca Raton: Taylor and Francis Group, LLC, 2010.

———. Hord. “(ISC)2 Website.” *Information Systems Security Certification Consortium*, at: http://www.isc2.org/aboutus/default.aspx (accessed May 27, 2010).

Traynor, Ben. “More on Today’s Gmail Issue.” *The Official Gmail Blog*. 9 September 2009, at: http://gmailblog.blogspot.com/2009/09/more-on-todays-gmail-issue.html (accessed June 13, 2010).

U.S. Computer Emergency Response Team, National Vulnerability Database. “*Vulnerability Summary for CVE-2009-3733*,” November 2, 2009, at: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3733 (accessed September 10, 2010).

Wald, Heather. "Cloud Computing for the Federal Community." *Information Assurance Newsletter*. Vol. 13, No. 2 (Spring 2010).

Williams, Alex. “Why the FBI’s Surveillance Proposal Could Be a Disaster for the Cloud.” *ReadWriteCloud*, September 28, 2010, at: http://www.readwriteweb.com/cloud/2010/09/why-fbi-surveillance-disaster.php (accessed October 1, 2010).

Wilshusen, Gregory C. *U.S. Government Accountability Office Report GAO-10-855T: Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing.* July 1, 2010, at: http://www.gao.gov/new.items/d10513.pdf (accessed October 7, 2010).

Yasin, Rutrel. “House panel questions cloud computing assumptions.” *Government Computer News*, July 1, 2010, at: http://gcn.com/articles/2010/07/01/congress-hearings-on-cloud-computing.aspx (accessed September 10, 2010).

Zetter, Kim. “Vulnerabilities Allow Attacker to Impersonate Any Website.” *Wired.com*, July 29, 2009, at: http://www.wired.com/threatlevel/2009/07/kaminsky/ (accessed July 23, 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dorothy E. Denning
   Naval Postgraduate School
   Monterey, California

4. Ted Lewis
   Naval Postgraduate School
   Monterey, California

5. Bret Michael
   Naval Postgraduate School
   Monterey, California

6. John Shea (John.Shea@osd.mil)
   NII/DoD CIO, Office of the DoD Chief Information Officer
   Arlington, Virginia

7. COL Kevin Foster, USA (Kevin.Foster@osd.mil)
   NII/DoD CIO, Office of the DoD Chief Information Officer
   Arlington, Virginia

8. Mr. John Kent (John.Kent@osd.mil)
   NII/DoD CIO, Office of the DoD Chief Information Officer
   Arlington, Virginia

9. Professor Mantak Shing (shing@nps.edu)
   Naval Postgraduate School
   Monterey, California

10. CAPT Sandra Jamshidi, USN (Sandra.Jamshidi@osd.mil)
    NII/DoD CIO, Office of the DoD Chief Information Officer
    Arlington, Virginia

11. Norma and Jack Antedomenico
    Tequesta, Florida